Upper Bounds on the Rate of Low Density Stabilizer Codes for the Quantum Erasure Channel

Nicolas Delfosse, Gilles Zémor
Institut de Mathématiques de Bordeaux UMR 5251, Université Bordeaux 1,
351, cours de la Libération, F-33405 Talence Cedex, France
Email: {Nicolas.Delfosse, Gilles.Zemor}@math.u-bordeaux1.fr

May 31, 2012

Abstract

Using combinatorial arguments, we determine an upper bound on achievable rates of stabilizer codes used over the quantum erasure channel. This allows us to recover the no-cloning bound on the capacity of the quantum erasure channel, $R \leq 1 - 2p$, for stabilizer codes: we also derive an improved upper bound of the form $R \leq 1 - 2p - D(p)$ with a function $D(p)$ that stays positive for $0 < p < 1/2$ and for any family of stabilizer codes whose generators have weights bounded from above by a constant – low density stabilizer codes.

We obtain an application to percolation theory for a family of self-dual tilings of the hyperbolic plane. We associate a family of low density stabilizer codes with appropriate finite quotients of these tilings. We then relate the probability of percolation to the probability of a decoding error for these codes on the quantum erasure channel. The application of our upper bound on achievable rates of low density stabilizer codes gives rise to an upper bound on the critical probability for these tilings.

1 Introduction

Low Density Parity Check (LDPC) codes are classical error-correcting codes originally introduced by Gallager [19]. They come with highly efficient local iterative decoding schemes, have been extensively studied and have proved very successful on a number of channels. Therefore, in the field of quantum communication and quantum computation, it is natural to look into the quantum analog of classical LDPC codes, which arguably are stabilizer codes with generators of bounded weight. We will call such codes low density stabilizer codes or, following others, refer to them somewhat loosely as quantum LDPC codes. These include a number of constructions of locally decodable quantum codes with a topological connection, starting with Kitaev's celebrated toric code [26], and other families among which surfaces codes [9], [37], color codes [7], [8], and other variants [35], [14]. Various generalizations to the quantum setting of classical LDPC codes have also been proposed, e.g. [1], [2], [13], [23], [32].

In the present work we are interested in the performance of quantum LDPC codes over the quantum erasure channel. Our motivation is inspired by the classical setting, in which the systematic study of LDPC codes for the classical erasure channel has led to a better understanding of the behaviour of LDPC codes for more complicated channels such as the binary symmetric channel and the Gaussian channel. This approach has hardly been attempted in

the quantum setting and it is not unreasonable to hope for similar returns in the long run. The quantum erasure channel, besides being simpler than the more universal depolarizing channel, is also a realistic channel [21]. Its capacity is known, it is $1-2p$ [5], however almost nothing is known about the performance of quantum LDPC codes over this channel. We would like to gain some understanding as to what are the code characteristics needed to achieve capacity.

We shall derive a bound on the achievable rate of stabilizer codes as a function of an upper bound on the weight of the generators of the stabilizer group. Equivalently, we will derive an upper bound on the decoding threshold on the erasure channel for quantum LDPC codes. This bound will yield the following result: any family of stabilizer codes that have stabilizer groups with generators of weight bounded by a constant, cannot achieve the capacity of the quantum erasure channel. This phenomenon is somewhat analogous to the classical setting [19] [10] where it is known that capacity achieving LDPC codes must have parity-check matrices with growing row weights.

Our result has an unexpected application to percolation theory. Given an infinite edge-transitive graph, a random subgraph, called the *open* subgraph is considered where every edge is declared open, independently of the others, with probability p. The central question in percolation theory is the determination of the critical probability p_c, which is the minimum value of p such that the open connected component of any given edge e is infinite with non zero probability. For most graphs, computing the critical probability exactly is usually quite difficult.

We are interested in the critical probability of graphs that make up regular tilings of the hyperbolic plane. The connection with quantum erasure correcting codes is that quotients of the infinite tiling of the hyperbolic plane yield finite graphs (more precisely combinatorial surfaces) that define quantum LDPC codes (surface codes): selecting a random erasure pattern for the finite code is the same as selecting a random subgraph of the finite graph, and the non-correctable erasure event is very close to the percolation event on the infinite graph. This connection was observed for the toric code [17], and this is why the erasure threshold of the toric code coincides with the critical probability $p_c = 1/2$ in the square lattice. We shall derive a bound on the erasure decoding threshold for surface codes that will lead to an upper bound on the critical probability p_c for hyperbolic tilings. To the best of our knowledge this is the sharpest presently known such upper bound.

The paper is organized as follows. After introductory and background material presented in Section 2, we derive an upper bound on achievable rates of stabilizer codes in Section 3. There are two main results in this section. The first is Theorem 3.5 which states that achievable rates of stabilizer codes satisfy a bound of the form $R \leq 1-2p-D(p)$ for a non-negative function $D(p)$. This enables one to recover the capacity bound $R \leq 1-2p$ for the quantum erasure channel for the particular case of stabilizer codes. It also enables one to derive improved bounds on achievable rates for particular classes of stabilizer codes. We derive such an improved bound in Theorem 3.8 for stabilizer codes with generators of bounded weight. In Section 4 we refine the above bound for a particular class of LDPC CSS codes that make up a family of surface codes. In Section 6 we apply the refined bound on achievable rates to percolation on hyperbolic lattices: the main result is Theorem 6.9 which is an upper bound on critical probabilities. Finally, an appendix regroups some technicalities necessary to complete formal proofs (Appendix A).

2 Background

A stabilizer code of parameters $[[n,k]]$ is a subspace of dimension 2^k of the space $\mathcal{H}^{\otimes n} = (\mathbb{C}^2)^{\otimes n}$. It is defined as the set of fixed points of an abelian group of Pauli operators. Below we go over notation and definitions. This material is quite well-known but we have felt the need to highlight the properties that we need, in particular because we shall make extensive use of linear algebra. For a more precise description of quantum information and quantum error-correcting codes, see Nielsen and Chuang [28] with a binary point of view close to the one that we adopt here, or the article of Calderbank, Rains, Shor and Sloane [12], for an $\mathbb{F}_4$ point of view.

2.1 Pauli groups

A quantum bit or qubit is a vector of $\mathcal{H} = \mathbb{C}^2$. It is the basic unit of quantum information. A sequence of n qubits lives in the space $\mathcal{H}^{\otimes n}$. The classical Pauli operators form a basis of the space of operators on $\mathcal{H}^{\otimes n}$.

Denote by I the identity matrix of size 2, $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $Y = iXZ$. These operators satisfy the following relations:

$$\begin{cases} X^2 = Y^2 = Z^2 = I, \\ XY = -YX = iZ, \\ YZ = -ZY = -iX, \\ ZX = -XZ = iY. \end{cases}$$

The Pauli group $\tilde{\mathcal{P}}_1$ for one qubit is the group generated by the matrices:

$$\tilde{\mathcal{P}}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

Remark that two different non-identity Pauli matrices always anti-commute.

The Pauli group $\tilde{\mathcal{P}}_n$ on n qubits is the multiplicative group of n-fold tensor products of errors of $\tilde{\mathcal{P}}_1$:

$$\tilde{\mathcal{P}}_n = \{i^a E_1 \otimes E_2 \otimes \cdots \otimes E_n \mid a = 0, 1, 2 \text{ or } 3 \text{ and } E_i = I, X, Y \text{ or } Z\}$$

The complex number i^a is the phase of the Pauli operator. An important consequence of this construction is the fact that two Pauli errors either commute or anti-commute. More precisely, given two errors E and E' of $\tilde{\mathcal{P}}_n$, we have:

$$EE' = (-1)^{f(E,E')} E'E,$$

where $f(E, E')$ is the number of components j such that E_j and E'_j are two different non-identity Pauli matrices. For example, the operators $I \otimes X \otimes Z$ and $X \otimes Y \otimes Z$ in $\tilde{\mathcal{P}}_3$ anti-commute because they anti-commute only in the second position. This fact is at the origin of syndrome measurement.

2.2 Stabilizer codes

A stabilizer group S is a commutative subgroup of $\tilde{\mathcal{P}}_n$ which doesn't contain $-I$. A stabilizer group is generated by a family of commuting Pauli operators: $S =< S_1, S_2, \ldots, S_r >$. Without

loss of generality, we can assume that these operators have phase 1. This ensure us that $-I$ is not in S.

Given S a stabilizer group of $\tilde{\mathcal{P}}_n$, the corresponding *stabilizer code* $C(S)$ is defined as the set of fixed points of the subgroup S in $\mathcal{H}^{\otimes n}$. Using the physical ket notation for vectors, we have:

$$C(S) = \{|\psi\rangle \in \mathcal{H}^{\otimes n} \mid s|\psi\rangle = |\psi\rangle, \forall s \in S\}.$$

This subspace is not trivial by construction of a stabilizer group. The integer n is the length of the quantum code. Assume that S is generated by r generators: $S =< S_1, S_2, \ldots, S_r >$ with $S_i \in \tilde{\mathcal{P}}_n$. We call the *stabilizer matrix* of $C(S)$ the matrix $\mathbf{H} \in \mathcal{M}_{r,n}(\{I, X, Y, Z\})$ with the i-th row representing the generator S_i. The coefficient $\mathbf{H}_{i,j}$ is the j-th component of S_i. For example, the quantum code associated with the 3 commuting generators $S_1 = (I \otimes X \otimes Z \otimes Y \otimes Z), S_2 = (Z \otimes Z \otimes X \otimes I \otimes Z)$, and $S_3 = (I \otimes Y \otimes Y \otimes Y \otimes Z)$ is described by the following stabilizer matrix:

$$\mathbf{H} = \begin{pmatrix} X & Z & I & I & Z \\ Z & X & X & Y & I \\ Y & Y & X & Y & Z \end{pmatrix}$$

A stabilizer code is completely defined by its stabilizer matrix, though different stabilizer matrices can define the same group and therefore the same code.

2.3 Syndrome of an error

Given $S =< S_1, S_2, \ldots, S_r >$ a stabilizer group of $\tilde{\mathcal{P}}_n$, assume that $|\psi\rangle \in C(S)$ is subjected to a Pauli error $E \in \tilde{\mathcal{P}}_n$. The vector $|\psi\rangle$ is corrupted to $E|\psi\rangle$. To recover the original quantum state, we measure the syndrome to obtain information on the error. The *syndrome* of $E \in \tilde{\mathcal{P}}_n$ is $\sigma(E) = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in \mathbb{F}_2^r$ defined by:

$$\sigma_i = \begin{cases} 0 \text{ if } E \text{ and } S_i \text{ commute} \\ 1 \text{ if } E \text{ and } S_i \text{ anti-commute} \end{cases}$$

Given the corrupted quantum state $E|\psi\rangle$ the syndrome of the error E can be measured. It satisfies $\sigma(EE') = \sigma(E) + \sigma(E')$. The syndrome of an error $s \in S$ which has no effect on the quantum code is $\sigma(s) = 0$.

2.4 Minimum distance of a stabilizer code

The phase i^a of a Pauli error $E \in \tilde{\mathcal{P}}_n$ does not play a role because we want to protect quantum states of $C(S)$, that is vectors of $C(S)$ defined up to multiplication by a non-zero complex number. Therefore, we will consider errors $E \in \mathcal{P}_n$ defined up to phases. In what follows, unless otherwise stated, the Pauli group will be the abelian quotient group:

$$\mathcal{P}_n = \tilde{\mathcal{P}}_n / \{\pm 1, \pm i\}.$$

Given E, E' in the group $\mathcal{P}_n$, we will say that they commute if they commute in the original group $\tilde{\mathcal{P}}_n$. This misuse of language is not problematic because commutation doesn't depend on the phase.

If we receive a quantum state $E|\psi\rangle$, where $|\psi\rangle$ is in the quantum code $C(S)$, we measure its syndrome $\sigma(E)$. We then apply to $E|\psi\rangle$ an error $\tilde{E}$ such that $\sigma(\tilde{E}) = \sigma(E)$. After this

process the quantum state is $\tilde{E}E|\psi\rangle$. It is corrupted by an error $\tilde{E}E$ of syndrome 0, because $\sigma(\tilde{E}E) = \sigma(\tilde{E}) + \sigma(E) = 0$. There are two types of error of zero syndrome. If $\tilde{E}E$ is in S, it fixes the quantum code and we have recovered the quantum state. Otherwise, the original quantum state is probably lost. Errors of zero syndrome that are not in S are called undetectable or *problematic* errors.

The above observation leads to the definition of the minimum distance d:

$$d = \min\{|E| \mid E \in \mathcal{P}_n \backslash S, \sigma(E) = 0\},$$

where $|E|$ is the weight of E, it is the number of non-identity components of E. In other words, d is the minimum weight of a problematic error. The set of errors of syndrome 0 in $\mathcal{P}_n$ is frequently denoted by $N(S)$, because it is the normalizer and the centralizer of the subgroup S in $\tilde{\mathcal{P}}_n$. Thus, the minimum distance is the minimum weight of an error of $N(S)\backslash S$.

2.5 Degeneracy

An essential feature of quantum coding theory that sets it appart from classical coding is degeneracy. It allows for the same decoding procedure to correct a large number of different errors. More precisely, all the errors of a coset $E.S$ can be corrected by the same error E. Indeed, assume that a state $|\psi\rangle$ of the quantum code is corrupted by an error Es, where $s \in S$. Then, after application of E, we recover the original quantum state because it is fixed by S. We have: $EEs|\psi\rangle = |\psi\rangle$. To correct an error $E \in \mathcal{P}_n$, it is sufficient to determine its coset $E.S$.

2.6 The $\mathbb{F}_2$-vector space structure, rank and dimension

The dimension of the quantum code $C(S)$ is 2^k, where $k = n - \operatorname{rank} S$. It is the number of encoded qubits. The quantity $\operatorname{rank} S$ is simply the rank of the abelian group S, i.e. the size of a minimum generating family. The *rate* of the quantum code is defined as $R = k/n$.

The Pauli group $\mathcal{P}_n$ can be seen as an $\mathbb{F}_2$-vector space of dimension $2n$, by the isomorphism:

$$\begin{aligned} \theta : \mathcal{P}_n &\longrightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n = \mathbb{F}_2^{2n} \\ X_i &\longmapsto (e_i|0) \\ Z_i &\longmapsto (0|e_i) \end{aligned}$$

where X_i is X on the i-th component and the identity on the other components. Errors Y_i and Z_i are defined similarly. The image of $Y_i = X_i Z_i$ is $\theta(X_i Y_i) = (e_i|e_i)$. For example, the operator $I \otimes X \otimes Y \otimes Z$ corresponds to the vector $(0110|0011)$. For this $\mathbb{F}_2$-vector space structure, the addition of vectors in $\mathbb{F}_2^{2n}$ corresponds to componentwise multiplication of Pauli errors.

By the isomorphism θ, subgroups of $\mathcal{P}_n$ are sent onto $\mathbb{F}_2$-linear subspaces of $\mathbb{F}_2^{2n}$. The rank of a subgroup of $\mathcal{P}_n$ is therefore also the dimension of the corresponding subspace. If $\mathbf{H}$ is a stabilizer matrix we will also write $\operatorname{rank} \mathbf{H}$ to denote the rank of its row-space, equivalently the rank of the associated stabilizer group. Note that we may choose a stabilizer matrix with a larger number r of rows than its rank.

We will find it convenient to keep the notation I, X, Y and Z for stabilizer matrices, but we stress the binary vector space structure that we will rely upon heavily in the next section.

With this vector space interpretation, the syndrome application:

$$\begin{aligned}\sigma : \mathcal{P}_n &\longmapsto \mathbb{F}_2^r \\ E &\longrightarrow \sigma(E)\end{aligned}$$

can be regarded as an $\mathbb{F}_2$-linear map.

2.7 The CSS construction

One of the most popular ways of constructing quantum codes is the Calderbank, Shor and Steane (CSS) construction [11, 34]. A CSS code is a stabilizer code constructed from a stabilizer group S such that:

$$S =< S_1, S_2, \ldots, S_{r_X}, S_{r_X+1}, \ldots, S_{r_X+r_Z} >$$

where $S_1, S_2, \ldots, S_{r_X}$ are included in $\{I, X\}^{\otimes n}$ and $S_{r_X+1}, S_{r_X+2}, \ldots, S_{r_X+r_Z}$ belong to $\{I, Z\}^{\otimes n}$. This simplifies commutation relations because two errors of $\{I, X\}^{\otimes n}$ automatically commute and it is similar in $\{I, Z\}^{\otimes n}$. In this case the stabilizer matrix $\mathbf{H}$ is decomposed into two stabilizer matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$. The matrix $\mathbf{H}_X$ is composed of r_X rows representing the stabilizers with coefficients in $\{I, X\}$ and the matrix $\mathbf{H}_Z$ is composed of r_Z rows which define the stabilizers with coefficients in $\{I, Z\}$.

Remark that the subgroup $\{I, X\}$ is isomorphic to $\mathbb{F}_2$, thus we can write the matrix $\mathbf{H}_X$ as a binary matrix. The same remark is also valid for $\mathbf{H}_Z$. By this last isomorphism, rows of the matrices can be seen as binary vectors of length n and the commutation relation between a row of $\mathbf{H}_X$ and a row $\mathbf{H}_Z$ corresponds to the orthogonality of these binary rows in $\mathbb{F}_2^n$.

Finally, a CSS code can be defined from two binary matrices $\mathbf{H}_X \in \mathcal{M}_{r_X,n}(\mathbb{F}_2)$ and $\mathbf{H}_Z \in \mathcal{M}_{r_Z,n}(\mathbb{F}_2)$ with orthogonality between rows of $\mathbf{H}_X$ and rows of $\mathbf{H}_Z$ in $\mathbb{F}_2^n$. The number of thus encoded qubits is:

$$k = n - \operatorname{rank} \mathbf{H}_X - \operatorname{rank} \mathbf{H}_Z,$$

because ranks of the binary matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ coincide with ranks of the corresponding groups. Denote by C_X the classical code $\operatorname{Ker} \mathbf{H}_X = \{c \in \mathbb{F}_2^n,\ \mathbf{H}_X\, {}^t c = 0\}$ and denote by C_Z the code $\operatorname{Ker} \mathbf{H}_Z$. The minimum distance of the quantum code is:

$$d = \inf\{w(x) \mid x \in C_X \backslash C_Z^{\perp} \cup C_Z \backslash C_X^{\perp}\},$$

where $w(x)$ is the Hamming weight of a binary vector.

Problematic errors. By the isomorphism of section 2.6, the error vector E can be seen as two simultaneous binary vectors, $\theta(E) = (E_X, E_Z)$. The error E has zero syndrome if and only if

$$E_X \in C_Z \ \text{ and } \ E_Z \in C_X \tag{1}$$

The error E is problematic if (1) holds together with the condition

$$E_X \notin C_X^{\perp} \ \text{ or } \ E_Z \notin C_Z^{\perp}. \tag{2}$$

3 Capacity of the quantum erasure channel

The capacity of a quantum channel is the highest rate of a family of quantum codes with an asymptotic zero error probability after decoding. Such a rate is called achievable. For the quantum erasure channel of erasure probability p, the capacity Q is $1-2p$ when $p \leq 1/2$ and it is zero above $1/2$. The upper bound

$$Q \leq 1 - 2p \tag{3}$$

comes from the no-cloning theorem, see for example [5]. Therefore, it doesn't rely on the quantum code structure. Since our purpose is to obtain improved capacity bounds for particular families of codes, namely quantum LDPC codes, we need to derive capacity from the code structure: our first step is to express achievable rates of stabilizer codes over the quantum erasure channel, as a function of their stabilizer matrices.

3.1 The quantum erasure channel

The quantum erasure channel admits several equivalent definitions. See for example [21], [20], [30]. As a completely positive trace preserving map, it is given by:

$$|\psi\rangle\langle\psi| \longmapsto (1-p)|\psi\rangle\langle\psi| + p|2\rangle\langle 2|$$

where $|\psi\rangle$ is a quantum state in $\mathcal{H}$ and the final state lives in $\mathbb{C}^3 = \mathcal{H} \oplus^{\perp} \mathbb{C}|2\rangle$. The vector $|2\rangle$ is orthogonal to the space $\mathcal{H}$, it corresponds to a lost qubit. In this paper, we will use the definition based on the Pauli operators which is well adapted to the stabilizer formalism. When we use the quantum erasure channel, each qubit is erased independently with probability p. An erased qubit is subjected to a random Pauli error I, X, Y or Z with equal probability $1/4$ and we know that this qubit is erased.

This description of the quantum erasure channel can be deduced from the definition as a completely positive trace preserving map. Indeed, the orthogonality between $|2\rangle$ and $\mathcal{H}$ allows us to measure the erased qubit. After, we replace the lost qubit $|2\rangle\langle 2|$ by a totally random qubit of density matrix $I/2$. This random state is the original qubit subjected to a random error I, X, Y or Z with equal probability. Therefore, we recover the second definition.

On n qubits, we denote by $\mathcal{E} \in \mathbb{F}_2^n$, the characteristic vector of the erased positions. Each component of the vector $\mathcal{E}$ follows a Bernoulli distribution of probability p. That is, the probability of a given vector $\mathcal{E} \in \mathbb{F}_2^n$ is $p^{|\mathcal{E}|}(1-p)^{n-|\mathcal{E}|}$. The qubit in position i is lost if and only if $\mathcal{E}_i = 1$. In this case, the quantum state is subjected to a random Pauli error $E \in \mathcal{P}_n$, which act trivially on the non-erased qubits: $E_i = I$ if $\mathcal{E}_i = 0$. We write this condition $E \subset \mathcal{E}$ and will say that erasure $\mathcal{E}$ *covers* the error E. Keep in mind that E is a Pauli operator with coefficients in $\{I, X, Y, Z\}$ and $\mathcal{E}$ is a binary vector, the shorthand notation $E \subset \mathcal{E}$ expresses just that the support of E is included in the set of erased positions. Note finally that given $\mathcal{E} \in \mathbb{F}_2^n$, all errors $E \subset \mathcal{E}$ occur with the same probability.

An encoded quantum state $|\psi\rangle$ is corrupted to a state $E|\psi\rangle$ by a random error E for which we have the additional knowledge $E \subset \mathcal{E}$. To recover the original quantum state, we compute the syndrome $\sigma \in \mathbb{F}_2^r$ and must deduce from the couple $(\mathcal{E}, \sigma)$ an error $\tilde{E} \subset \mathcal{E}$. To correct the effect of E we apply $\tilde{E}$ and the final state is $\tilde{E}E|\psi\rangle$. If the errors E and $\tilde{E}$ are in the same coset modulo S, then $\tilde{E}E$ is a stabilizer of the quantum code. Thus the final quantum state is the original state. When $\tilde{E}$ is not equivalent to E, we will not, in general, recover the

quantum state. Note that in this case $\tilde{E}E$ is a problematic error and $\tilde{E}E \subset \mathcal{E}$. When this happens, i.e. when the erasure vector covers a problematic error, we will say that we have a *non-correctable* erasure: otherwise the erasure is correctable.

Non-correctable erasures in the CSS case. From the characterization (1) and (2) of problematic errors, we obtain the simple characterisation of a non-correctable erasure in the CSS case.

Proposition 3.1. *Let* $\mathbf{H} = \begin{pmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{pmatrix}$ *be the stabilizer matrix of a CSS code, and let* C_X *and* C_Z *be the corresponding classical binary codes. The erasure vector* $\mathcal{E} \in \mathbb{F}_2^n$ *is non-correctable if and only if there exists a binary vector* v *whose support is included in the support of* $\mathcal{E}$ *and such that*

$$v \in C_X \setminus C_Z^{\perp} \;\; or \;\; v \in C_Z \setminus C_X^{\perp}.$$

3.2 An example of a non-correctable erasure

As an example of the general case, consider the stabilizer code defined by the matrix:

$$\mathbf{H} = \begin{pmatrix} I & X & Z & Y & Z \\ Z & Z & X & I & Z \\ I & Y & Y & Y & Z \end{pmatrix}$$

If the erasure is $\mathcal{E} = (0, 1, 1, 0, 0)$, there are $2^{2|\mathcal{E}|} = 2^4$ possible errors:

$$\{E \in \mathcal{P}_n \mid E \subset \mathcal{E}\} = \{X_2^{a_2} Z_2^{b_2} X_3^{a_3} Z_3^{b_3} \mid a_i, b_i \in \mathbb{F}_2\},$$

where the error X_i is the error with i-th component X and which is the identity outside i. The operator Z_i is defined similarly and Y_i is the error $X_i Z_i$.
Let us focus our attention on the "erased matrix"

$$\mathbf{H}_{\mathcal{E}} = \begin{pmatrix} X & Z \\ Z & X \\ Y & Y \end{pmatrix}$$

which is the submatrix of $\mathbf{H}$ whose columns are the columns indexed by the erased positions. It is natural to introduce this matrix because the syndrome of an error included in the erasure $\mathcal{E}$ depends only on these columns. We remark that the third row of this matrix is the product of the first two rows. Thus, the syndrome $u \in \mathbb{F}_2^3$ of an error $E \subset \mathcal{E}$ satisfies $u_3 = u_1 + u_2$. It depends only on the first two rows of $\mathbf{H}_{\mathcal{E}}$. Therefore, there are 2^2 different syndrome values for errors E that are covered by the erasure.
Now let us look at the remaining columns. The non-erased submatrix $\mathbf{H}_{\bar{\mathcal{E}}}$ is:

$$\mathbf{H}_{\bar{\mathcal{E}}} = \begin{pmatrix} I & Y & Z \\ Z & I & Z \\ I & Y & Z \end{pmatrix}.$$

Assume that E and E' are two errors included in $\mathcal{E}$, which are in the same degeneracy class. That is, they differ by right-multiplication by an error $s \in S$. The restriction of the error $s = EE'$ to $\bar{\mathcal{E}}$ is the identity. The rank of this submatrix is $\operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}} = 2$ because the first row and the third row are identical. Therefore, we have two possibilities for s: either $s = I^{\otimes 5}$

or $s = S_1 S_3 = I \otimes Z \otimes X \otimes I \otimes I$. There are two errors in each degeneracy class and four possible syndrome values: therefore, if there were no problematic error included in $\mathcal{E}$ the total number of errors included in $\mathcal{E}$ would be $2 \times 4 = 2^3$, but we have seen that it actually is 2^4. This erasure is not correctable.

3.3 Two enumeration lemmas

We will pursue the preceding approach. Our strategy is to determine the cardinalities of two sets of Pauli errors:

- $N(S)_\mathcal{E} = \{E \in N(S) \mid E \subset \mathcal{E}\}$,
  recall that $N(S)$ is the set of Pauli errors of syndrome 0.
- $S_\mathcal{E} = \{s \in S \mid s \subset \mathcal{E}\}$.

We will use the submatrices introduced in the above example.

The random submatrix $\mathbf{H}_\mathcal{E}$: Let $\mathbf{H}$ be a matrix of a stabilizer code. With an erasure $\mathcal{E} \in \mathbb{F}_2^n$, we associate the submatrix $\mathbf{H}_\mathcal{E}$ of the stabilizer matrix $\mathbf{H} \in \mathcal{M}_{r,n}(\mathcal{P}_1)$ composed of the columns of the erased qubits. This is the submatrix of the columns of index i such that $\mathcal{E}_i = 1$. Similarly $\mathbf{H}_{\bar{\mathcal{E}}}$ is the matrix of the non-erased qubits, corresponding to the conjugate $\bar{\mathcal{E}}$ of $\mathcal{E}$ defined by: $\bar{\mathcal{E}}_i = \mathcal{E}_i + 1$.

Lemma 3.2. *Let S be a stabilizer group of matrix $\mathbf{H} \in \mathcal{M}_{r,n}$. The set $N(S)_\mathcal{E}$ is an $\mathbb{F}_2$-vector space of dimension $2|\mathcal{E}| - \operatorname{rank} \mathbf{H}_\mathcal{E}$.*

Proof. The $\mathbb{F}_2$-linear structure of the Pauli group $\mathcal{P}_n$ has been detailed in Section 2.6. The syndrome is an $\mathbb{F}_2$-linear map from $\mathcal{P}_n$ to $\mathbb{F}_2^r$. Its restriction $\sigma_\mathcal{E}$ to the space of Pauli errors included in $\mathcal{E}$ is also an $\mathbb{F}_2$-linear map. The subspace $N(S)_\mathcal{E}$ is simply the kernel of $\sigma_\mathcal{E}$. Its dimension is $2|\mathcal{E}| - \dim \operatorname{Im} \sigma_\mathcal{E}$. The restricted syndrome function $\sigma_\mathcal{E}$ depends only on the submatrix $\mathbf{H}_\mathcal{E}$. It is straightforward to see that the dimension of its image is the rank of $\mathbf{H}_\mathcal{E}$. □

Lemma 3.3. *Let S be a stabilizer group of matrix $\mathbf{H} \in \mathcal{M}_{r,n}$. The set $S_\mathcal{E}$ is an $\mathbb{F}_2$-vector space of dimension* $\operatorname{rank} \mathbf{H} - \operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}}$.

Proof. The set $S_\mathcal{E}$ is the kernel of the $\mathbb{F}_2$-linear map:

$$\begin{aligned} S &\longrightarrow \{E \in \mathcal{P}_n \mid E \subset \mathcal{E}\} \\ s &\longmapsto s_{|\bar{\mathcal{E}}} \end{aligned}$$

By definition of the rank, the image of this application is a space of dimension $\operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}}$, and the group S has dimension $\operatorname{rank} \mathbf{H}$. Therefore, $\dim S_\mathcal{E} = \operatorname{rank} \mathbf{H} - \operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}}$. □

From the lemmas, there are $2^{\operatorname{rank} \mathbf{H}_\mathcal{E}}$ different syndromes and in each coset modulo S there are $2^{\operatorname{rank} \mathbf{H} - \operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}}}$ errors included in $\mathcal{E}$. Therefore the number of correctable error patterns is $2^{\operatorname{rank} \mathbf{H} + \operatorname{rank} \mathbf{H}_\mathcal{E} - \operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}}}$, and since there are $2^{2|\mathcal{E}|}$ error vectors covered by $\mathcal{E}$, the erasure vector $\mathcal{E}$ can be corrected only if:

$$2|\mathcal{E}| \leq \operatorname{rank} \mathbf{H} + \operatorname{rank} \mathbf{H}_\mathcal{E} - \operatorname{rank} \mathbf{H}_{\bar{\mathcal{E}}}. \tag{4}$$

The rank of $\mathbf{H}$ is $\operatorname{rank}\mathbf{H} = (1-R)n$ where R is the rate of the quantum code. When $p \leq 1/2$, there are typically more non-erased coordinates than erased ones, and it is reasonable to expect that the larger matrix $\mathbf{H}_{\bar{\mathcal{E}}}$ has a higher rank than the smaller matrix $\mathbf{H}_{\mathcal{E}}$. Equation (4) therefore becomes simply $2|\mathcal{E}| \leq \operatorname{rank}\mathbf{H}$ and the typical weight of an erasure being $|\mathcal{E}| = np$, we obtain:

$$R \leq 1 - 2p$$

which recovers (3) for the class of stabilizer codes. In the next section we will make this informal argument rigorous and pave the way for improvements for particular classes of quantum codes.

3.4 A combinatorial bound on the capacity

Now, we will give a rigorous proof using an entropic formulation of this idea and Fano's inequality.

Recall that a rate $R \in [0,1]$ is achievable if there exists a family of codes of rates R_t converging to R with vanishing error probability after decoding. Denote expectation by $\mathbb{E}$. Let $(\mathbf{H}_t)_t$ be a sequence of stabilizer matrices and denote by n_t the length of the code defined by the matrix $\mathbf{H}_t$.

Definition 3.4. *The rank difference function D associated with the sequence $(\mathbf{H}_t)_t$ of stabilizer matrices is $D(p) = \limsup_t \Delta_t(p)$ where :*

$$\Delta_t(p) = \frac{\mathbb{E}_p[\operatorname{rank}\mathbf{H}_{t,\bar{\mathcal{E}}} - \operatorname{rank}\mathbf{H}_{t,\mathcal{E}}]}{n_t}.$$

Theorem 3.5. *Achievable rates of a sequence of stabilizer codes of matrices $(\mathbf{H}_t)_{t\in\mathbb{N}}$, over the quantum erasure channel of probability p, satisfy:*

$$R \leq 1 - 2p - D(p).$$

where $D(p)$ is the rank difference function of the family $(\mathbf{H}_t)_t$.

Proof. We shall apply the classical Fano inequality, see for example [15]. Recall that if X, Y and $\hat{X}$ are any three random variables such that $\hat{X}$ depends only on Y, then Fano's inequality states:

$$P_{err} := \mathbb{P}(\hat{X} \neq X) \geq \frac{H(X|Y) - 1}{\log(|\mathcal{X}|)}.$$

where X takes its values in $\mathcal{X}$.

Over the quantum erasure channel, $\mathcal{E}$ is the erasure vector random variable with distribution $\mathbb{P}(\mathcal{E} = v) = p^{|v|}(1-p)^{n-|v|}$. The error random variable E is uniformly distributed among the errors acting on the erased components. We apply Fano's inequality when X is the information we need to recover the quantum state, namely the coset $E.S$ of the Pauli error vector E. We set the variable Y to be the couple $Y = (\mathcal{E}, \Sigma)$ where $\mathcal{E}$ is the erasure vector random variable defined above and $\Sigma = \sigma(E)$ is the syndrome of E. The variable $\hat{X}$ is the best possible estimation of X given Y, meaning here that the decoding error probability P_{err} is the probability to have $X \neq \hat{X}$.

The conditional entropy is decomposed as:

$$H(X|\mathcal{E},\Sigma) = \sum_{v,y} \mathbb{P}\big((\mathcal{E},\Sigma) = (v,y)\big) H(X|\mathcal{E} = v, \Sigma = y).$$

We have:

$$H(X|\mathcal{E}=v,\Sigma=y) = 2|v| - \operatorname{rank}\mathbf{H} + \operatorname{rank}\mathbf{H}_{\bar{v}} - \operatorname{rank}\mathbf{H}_v,$$

the proof of which is detailed in Lemma 3.6 below. We see that the value of $H(X|\mathcal{E}=v,\Sigma=y)$ is independent of y, thus we have:

$$\begin{aligned} H(X|\mathcal{E},\Sigma) &= \sum_v \mathbb{P}(\mathcal{E}=v)\big(2|v| - \operatorname{rank}\mathbf{H} - \operatorname{rank}\mathbf{H}_v + \operatorname{rank}\mathbf{H}_{\bar{v}}\big) \\ &= 2np - \operatorname{rank}\mathbf{H} + \mathbb{E}_p(\operatorname{rank}\mathbf{H}_{\bar{\mathcal{E}}} - \operatorname{rank}\mathbf{H}_{\mathcal{E}}). \end{aligned}$$

The random variable $X = E.S$ takes on values in the quotient group $\mathcal{X} = \mathcal{P}_n/S$. This quotient group is composed of $|\mathcal{X}| = 2^{2n-\operatorname{rank}\mathbf{H}}$ classes. From Fano's inequality we get, upperbounding the denominator by $2n - \operatorname{rank}\mathbf{H} \leq 2n$,

$$P_{err} \geq \frac{2np - \operatorname{rank}\mathbf{H} + \mathbb{E}_p(\operatorname{rank}\mathbf{H}_{\bar{\mathcal{E}}} - \operatorname{rank}\mathbf{H}_{\mathcal{E}}) - 1}{2n}$$

The rate of the quantum code is $R = 1 - \operatorname{rank}\mathbf{H}/n$. If the error probability goes to zero, then the rate of the quantum code family satisfies:

$$\limsup R \leq 1 - 2p - D(p).$$

□

Lemma 3.6. *Let S be a stabilizer group of matrix $\mathbf{H}$. The conditional entropy of $X = E.S$ given $\mathcal{E} = v$ and $\Sigma = y$ is:*

$$H(X|\mathcal{E}=v,\Sigma=y) = 2|v| - \operatorname{rank}\mathbf{H} + \operatorname{rank}\mathbf{H}_{\bar{v}} - \operatorname{rank}\mathbf{H}_v,$$

when the probability to have $\mathcal{E} = v$ and $\Sigma = y$ is non zero.

Proof. Recall that given the erasure $\mathcal{E}$, the distribution of E is uniform inside the support of $\mathcal{E}$. Therefore, the probability of a coset $E.S$, assuming that the erasure is $\mathcal{E} = v$ and the syndrome is $\Sigma = y$, is:

$$\mathbb{P}(X = E.S|\mathcal{E}=v,\Sigma=y) = \frac{|\{P \in E.S \mid P \subset v, \sigma(P) = y\}|}{|\{P \in \mathcal{P}_n \mid P \subset v, \sigma(P) = y\}|}.$$

When this probability is non-zero, by linearity, (multiply by an operator $T \subset v$ of syndrome y), we can assume that $y = 0$. The set in the denominator is the subgroup $N(S)_v$ and the set in the numerator is a coset of the subgroup S_v. Applying Lemmas 3.2 and 3.3 we have:

$$\mathbb{P}(X = E.S|\mathcal{E}=v,\Sigma=y) = \frac{|S_v|}{|N(S)_v|} = 2^{-2|v|+\operatorname{rank}\mathbf{H}-\operatorname{rank}\mathbf{H}_{\bar{v}}+\operatorname{rank}\mathbf{H}_v}.$$

whence

$$H(X|\mathcal{E}=v,\Sigma=y) = 2|v| - \operatorname{rank}\mathbf{H} + \operatorname{rank}\mathbf{H}_{\bar{v}} - \operatorname{rank}\mathbf{H}_v.$$

□

The following corollary proves the efficiency of our method. We recover the upper bound given by the capacity of the quantum erasure channel [5]. This bound is deduced only from combinatorial properties of stabilizer codes. It doesn't involve the no-cloning theorem.

Corollary 3.7. *Achievable rates of a sequence of stabilizer codes of matrices $(\mathbf{H}_t)_{t\in\mathbb{N}}$, over the quantum erasure channel of probability p, satisfy:*

$$R \leq 1 - 2p,$$

when $p \leq 1/2$.

Proof. To prove the corollary, it suffices to remark that $\Delta_t(p)$ in Theorem 3.5 is non-negative when $p \leq 1/2$. Observe that we can write the function Δ_t as:

$$\Delta_t(p) = \phi_t(1-p) - \phi_t(p),$$

where $\phi_t(p) = \mathbb{E}_p(\operatorname{rank} \mathbf{H}_{t,\mathcal{E}})/n_t$. It is intuitively clear and it is formally stated and proved in Appendix A (Proposition A.3) that ϕ_t is an increasing function of p. The corollary follows. □

Our goal is now to improve on Corollary 3.7 by finding non-zero lower bounds on $D(p)$. This cannot be done for stabilizer codes in general since they are known to achieve capacity of the quantum erasure channel, but we can obtain such improvements for *sparse* quantum codes, i.e. codes that have sparse stabilizer matrices. Our most general result in this direction is Theorem 3.8 below. It is somewhat reminiscent of an upper bound on achievable rates of classical LDPC codes for the classical erasure channel [31].

3.5 Reduction to the study of the mean rank of a random submatrix of the stabilizer matrix

Theorem 3.8. *Let $\mathcal{C}$ be any family of stabilizer codes of rates at least R and achieving vanishing decoding error probability over the quantum erasure channel of erasure probability p. Suppose furthermore that every code $C \in \mathcal{C}$ has a set of generators of its stabilizer group whose weights are all upper bounded by m. Then we have:*

$$R \leq (1-2p)\frac{1-(1-p)^{m-1}}{1-(1-2p)(1-p)^{m-1}}.$$

Method: Let $\mathbf{H}$ be a stabilizer matrix and set $\phi(p) = \mathbb{E}_p(\operatorname{rank} \mathbf{H}_{\mathcal{E}})/n$. Denote by Δ the function $\Delta(p) = \phi(1-p) - \phi(p)$. To apply Theorem 3.5 we need a lower bound on $\Delta(p)$. Because the function ϕ is concave, any upper bound $\phi(p) \leq M(p)$ implies the lower bound on Δ:

$$\Delta(p) \geq \frac{1-2p}{1-p}\left(\frac{\operatorname{rank} \mathbf{H}}{n} - M(p)\right). \tag{5}$$

The formal proof of the concavity of ϕ and of (5) is somewhat technical and not necessary to the understanding of the main ideas, therefore it is placed in Appendix A (Proposition A.5).

Proof of Theorem 3.8. Let $\mathbf{H}$ be a stabilizer matrix of a code $C \in \mathcal{C}$. Set $\phi(p) = \mathbb{E}_p(\operatorname{rank} \mathbf{H}_{\mathcal{E}})/n$. Let $\mathbf{h}^0_{\mathcal{E}}$ stand for the number of zero rows in the random submatrix $\mathbf{H}_{\mathcal{E}}$. We have:

$$\begin{aligned}\phi(p) \leq & \frac{1}{n}\left[\operatorname{rank} \mathbf{H} - \mathbb{E}_p(\mathbf{h}^0_{\mathcal{E}})\right] \\ \leq & \frac{\operatorname{rank} \mathbf{H}}{n} - \frac{\operatorname{rank} \mathbf{H}}{n}(1-p)^m.\end{aligned}$$

Applying (5) we get:

$$\Delta(p) \geq \frac{1-2p}{1-p}\frac{\operatorname{rank}\mathbf{H}}{n}(1-p)^m \geq \frac{1-2p}{1-p}(1-R)(1-p)^m.$$

From Theorem 3.5 we now have:

$$R \leq 1-2p-(1-R)(1-2p)(1-p)^{m-1}$$

and the result follows after rearranging. □

As an example let us consider the family of *color codes* [7]. Color codes are defined from a trivalent tiling of a surface by faces and the associated stabilizer matrices have rows of weight bounded by the maximum length (number of edges) of a face. Hence Theorem 3.8 applies to this family that cannot be capacity-achieving if the faces stay with bounded length.

4 Achievable rates of $(2, m)$ CSS codes

We now turn to deriving a refined upper bound on achievable rates of a particular family of quantum LDPC codes. Let us say that a binary matrix is of type $(2, m)$ if every one of its rows is of weight m and every column is of weight 2. We shall say that a quantum code is a $(2, m)$ CSS code if its stabilizer matrix $\mathbf{H}$ decomposes in two matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$, *each of which is a* $(2, m)$ *matrix*.

4.1 The 2-complex associated to a $(2, m)$ CSS code

The matrix $\mathbf{H}_X$, viewed as a binary matrix, can be seen as the incidence matrix of a finite graph G_X. The vertex set V of the graph G_X is defined as the set of rows of $\mathbf{H}_X$, and two vertices i and i' are declared to be incident if there is column j such that there are 1's in positions (i, j) and (i', j). The Edge set of the graph G_X can therefore be indexed by the columns of $\mathbf{H}_X$. The constant row weight m of $\mathbf{H}_X$ means that the graph G_X is regular (every vertex has m neighbours).

Recall that the classical code C_X is the set of vectors of $\mathbb{F}_2^n$ orthogonal to the rows of $\mathbf{H}_X$. The code C_X is generated by the vectors whose supports coincide with cycles of the graph G_X (actually C_X is *exactly* the set of cycles of G_X when one allows cycles to be non-connected subgraphs) and C_X is classically called the *cycle code* of the associated graph G_X.

If the graph G_X has n edges, the dimension of the code C_X is given by:

Lemma 4.1. *We have* $\dim C_X = n - |V| + \kappa_X$ *where* κ_X *is the number of connected components of* G_X.

This is a classical result, see for example [6].

Since the rows of $\mathbf{H}_Z$ are orthogonal to the rows of $\mathbf{H}_X$, the supports of the rows of $\mathbf{H}_Z$ are cycles of the graph G_X. The graph G_X together with the set of supports of the rows of $\mathbf{H}_Z$ is called a 2-complex, and the supports of the rows of $\mathbf{H}_Z$ are particular cycles that are called *faces*. That $\mathbf{H}_Z$ is a $(2, m)$ matrix means that every edge is incident to exactly two faces.

In the same way that the matrix $\mathbf{H}_X$ defines a graph G_X, the matrix $\mathbf{H}_Z$ defines a graph G_Z, which together with $\mathbf{H}_X$ also makes up a 2-complex. The two complexes are said to be dual to each other: faces are vertices of the dual complex.

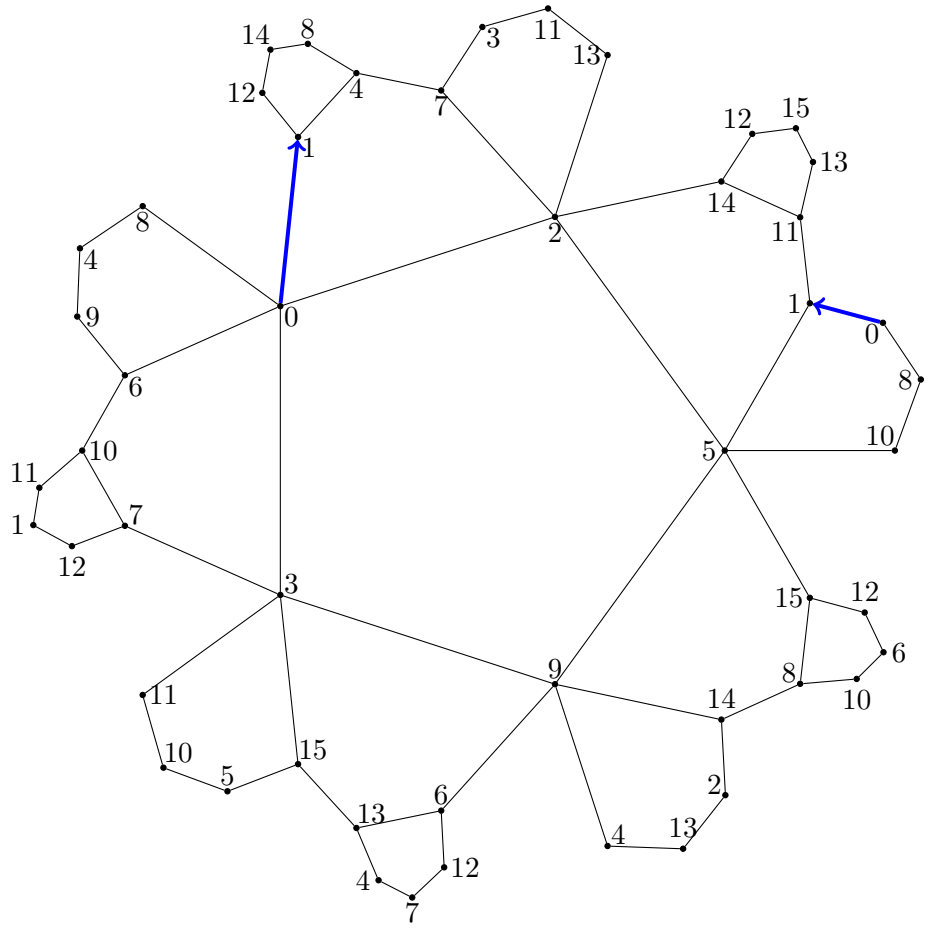

Figure 1: An example of self-dual 5-regular tiling of a surface of genus 4 composed of 16 vertices, 40 edges and 16 faces. Each face is represented once. Vertices are represented several times to allow this planar representation. Each boundary edge is represented twice. multiple replicas of vertices and edges are identified to create the surface. In bold the identification of the edges $\{0, 1\}$.

We shall say that the $(2, m)$ CSS code (or equivalently the associated 2-complex) is *proper* if the two graphs G_X and G_Z are connected and have girth (smallest cycle size) equal to m.

It is not immediate that proper $(2, m)$ CSS codes even exist, and the existence of families of $(2, m)$ CSS codes with growing minimum distance is even less obvious. One way of coming up with such families is through the construction of combinatorial surfaces. the associated $(2, m)$ CSS codes are a highly regular instance of *surface codes* [9, 37]. An example of such a surface is given on Figure 1 for $m = 5$. The associated $(2, 5)$ matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ are given on Figure 2. It is the smallest $(2, 5)$ CSS code we have found such that the associated graphs G_X and G_Z are both connected and simple (without multiple edges). The only method we know of that allows the construction of proper $(2, m)$ CSS codes involves sophisticated number-theoretic arguments and combinatorial surfaces. We shall take up this matter in Section 6 where upper bounds on the achievable rate of quantum $(2, m)$ CSS codes lead to upper bounds on the critical probability for associated families of infinite tilings.

$$\mathbf{H}_X = \begin{pmatrix} 0 & 1 & 2 & 3 & 8 \\ 1 & 4 & 5 & 11 & 20 \\ 2 & 6 & 7 & 14 & 25 \\ 0 & 9 & 10 & 18 & 28 \\ 5 & 12 & 13 & 22 & 32 \\ 4 & 7 & 15 & 21 & 31 \\ 3 & 16 & 17 & 27 & 36 \\ 6 & 10 & 13 & 19 & 23 \\ 8 & 12 & 24 & 33 & 38 \\ 9 & 15 & 17 & 22 & 26 \\ 16 & 19 & 21 & 24 & 29 \\ 11 & 28 & 29 & 30 & 35 \\ 20 & 23 & 27 & 34 & 39 \\ 14 & 32 & 35 & 36 & 37 \\ 25 & 26 & 30 & 33 & 34 \\ 18 & 31 & 37 & 38 & 39 \end{pmatrix} \qquad \mathbf{H}_Z = \begin{pmatrix} 0 & 2 & 7 & 9 & 15 \\ 1 & 2 & 5 & 6 & 13 \\ 0 & 3 & 10 & 16 & 19 \\ 1 & 4 & 8 & 21 & 24 \\ 3 & 8 & 12 & 17 & 22 \\ 4 & 7 & 11 & 25 & 30 \\ 5 & 12 & 20 & 33 & 34 \\ 6 & 10 & 14 & 28 & 35 \\ 9 & 17 & 18 & 36 & 37 \\ 11 & 19 & 20 & 23 & 29 \\ 13 & 23 & 27 & 32 & 36 \\ 14 & 22 & 25 & 26 & 32 \\ 15 & 26 & 31 & 33 & 38 \\ 16 & 24 & 27 & 38 & 39 \\ 18 & 21 & 28 & 29 & 31 \\ 30 & 34 & 35 & 37 & 39 \end{pmatrix}$$

Figure 2: Two matrices of size 16×40 defining a $(2, 5)$ CSS code of parameters $[[40, 10, 4]]$. Columns are indexed by the integers $\{0, 2, \ldots, 39\}$ and rows are described by their supports. This code is the surface code defined from the 2-complex of Figure 1.

4.2 Reduction to the study of the mean number of connected components in the subgraph of a graph

Recall from our proof method described in Section 3.5 that our objective is to find an upper bound on the function $\phi(p) = \mathbb{E}_p(\operatorname{rank} \mathbf{H}_\mathcal{E})/n$ for a stabilizer matrix $\mathbf{H}$. Since we are dealing with the stabilizer matrix $\mathbf{H} = \begin{pmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{pmatrix}$ of a CSS code, we have $\phi(p) = \phi_X(p) + \phi_Z(p)$ where $\phi_X(p) = \mathbb{E}_p(\operatorname{rank} \mathbf{H}_{X,\mathcal{E}})/n$ and $\phi_Z(p) = \mathbb{E}_p(\operatorname{rank} \mathbf{H}_{Z,\mathcal{E}})/n$. Recall that the two matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ are $(2, m)$ matrices. Our problem is therefore to bound from above the mean rank of random submatrix of a fixed binary $(2, m)$ matrix.

In the rest of this section, let $H \in \mathcal{M}_{r,n}$ therefore stand for a binary matrix of type $(2, m)$. We create the submatrix $H_\mathcal{E}$ by keeping every column of H with probability p and independently of the others.

The random subgraph $G_\mathcal{E}$: As described in section 4.1 we can regard the matrix H as the incidence matrix of a graph G with vertex set V.

Given the random vector $\mathcal{E} \in \mathbb{F}_2^n$, we denote by $G_\mathcal{E}$ the subgraph of G of incidence matrix $H_\mathcal{E}$. Assume that each component of $\mathcal{E}$ is 1 with probability p and 0 with probability $1 - p$, independently. Then, the graph $G_\mathcal{E}$ is the random subgraph of G with unchanged vertex set, and obtained by taking each edge, independently, with probability p. In other words, taking a random submatrix $H_\mathcal{E}$ of H corresponds to taking a random subgraph $G_\mathcal{E}$ of G. For the random subgraph $G_\mathcal{E}$, Lemma 4.1 translates into:

Lemma 4.2. *If H is a binary $(2, m)$ matrix with $|V|$ rows, then $|V| - \operatorname{rank} H_\mathcal{E}$ is equal to the number $\kappa_\mathcal{E}$ of connected components of the subgraph $G_\mathcal{E}$. That is:*

$$\operatorname{rank} H_\mathcal{E} = |V| - \kappa_\mathcal{E}.$$

4.3 Bound on the mean number of connected components in the graph

From Lemma 4.2, the mean rank of the submatrix $H_{\mathcal{E}}$ can be expressed as a function of the expected number of connected components of the graph $G_{\mathcal{E}}$:

$$\frac{\mathbb{E}_p(\operatorname{rank} H_{\mathcal{E}})}{n} = \frac{|V|}{n} - \frac{\mathbb{E}_p(\kappa_{\mathcal{E}})}{n} \tag{6}$$

If we upper bound $\mathbb{E}_p(\operatorname{rank} H_{\mathcal{E}})/n$ by writing that $\mathbb{E}_p(\kappa_{\mathcal{E}})$ is lower bounded by the expected number of isolated vertices, we will simply recover Theorem 3.8. We will proceed to derive a more precise lower bound by enumerating larger connected components.

Assuming that the m-regular graph G constructed from the matrix H has no small cycles, it looks like the m-regular tree G_m in any sufficiently small neighbourhood. Thus, for our enumeration problem, we introduce the number a_k of subtrees of G_m, with k edges, containing a fixed vertex x of G_m. We will use a generating function approach: for background, two classical references on this subject are [18] and [36].

The generating function for rooted trees: Let G_m be the m-regular tree and let x be a fixed vertex of G_m called a root. Let us define the generating function for rooted tree of degree m as the real function:

$$T_m(z) = \sum_{k \geq 0} a_k z^k,$$

where a_k is the number of subtrees of G_m, with k edges, containing the root x. To compute this generating function, it is useful to introduce the auxiliary generating function.

$$T_m^1(z) = \sum_{k \geq 0} b_k z^k,$$

where b_k is the number of subtrees $\mathcal{T}$ of G_m such that :

- $\mathcal{T}$ is composed of k edges,
- the root x is included in $\mathcal{T}$,
- $\mathcal{T}$ contains a fixed edge $\{x, y\}$ among edges incident to x, and no other edge incident to x is contained in $\mathcal{T}$.

This generating function doesn't depend on the particular choice of the edge x, y, by regularity of G_m. The function $T_1(z)$ is sometimes called the generating function of planted rooted subtrees, since x has degree one in such a subtree.

Coefficients b_k can be computed easily using the Lagrange inversion Theorem [18] because T_m^1 satisfies:

$$T_m^1(z) = z(1 + T_m^1(z))^{m-1}$$

This formula comes from the fact that every vertex of the tree except the root x has $m-1$ sons. We get:

$$b_k = \frac{1}{k}\binom{k(m-1)}{k-1}.$$

Then, the computation of the a_k follows from the expression of T_m as a function of T_m^1.

$$T_m(z) = (1 + T_m^1(z))^m.$$

To see this formula remark that a subgraph of G_m containing the root x can be decomposed into at m planted subtrees of root x. This method allows the computation of a large number of coefficients a_k using symbolic computation software.

We can now state an upper bound on the expected rank of the submatrix $H_{\mathcal{E}}$ involving the numbers a_k.

Proposition 4.3. *If H is a binary $(2, m)$ matrix whose associated graph G has girth (smallest cycle size) at least $\delta + 2$, then*

$$\frac{\mathbb{E}_p(\operatorname{rank} H_{\mathcal{E}})}{n} \leq \frac{2}{m}\big(1 - (1-p)^m S_\delta(p(1-p)^{m-2})\big),$$

where $S_\delta(z) = \sum_{k=0}^{\delta} \frac{a_k}{k+1} z^k$ and the a_k are the coefficients of the generating function T_m.

Proof. From (6) we want a lower bound on the expected number of connected components in the graph $G_{\mathcal{E}}$.

The graph $G_{\mathcal{E}}$ is constructed from the edge set of G by choosing each edge, independently, with probability p. Let us compute the expected number of connected components with 0 edges. This is the average number of isolated points in the random subgraph $G_{\mathcal{E}}$. Denote by X_0 the random variable which associate with a random vector $\mathcal{E}$, the number of isolated points in $G_{\mathcal{E}}$. We can write $X_0(\mathcal{E}) = \sum X_v(\mathcal{E})$ where: $X_v(\mathcal{E}) = 1$ if the vertex v is isolated in $G_{\mathcal{E}}$ and $X_v(\mathcal{E}) = 0$ otherwise. By linearity of expectation, we have:

$$\mathbb{E}(X_0) = \sum_v \mathbb{E}(X_v) = \sum_v \mathbb{P}(X_v = 1) = |V|(1-p)^m.$$

Indeed, each vertex is bordered by m edges, therefore $\mathbb{P}(X_v = 1) = (1-p)^m$, for every vertex v.

This idea can be used with components of size (number of edges) $k \leq \delta$. For C a k-edge connected subgraph of G, let X_C denote the random variable equal to 1 if C is a connected component of the random graph $G_{\mathcal{E}}$, and 0 otherwise. The average number of connected components of size k is:

$$\mathbb{E}(X_k) = \sum_{\substack{C \text{ connected} \\ \text{subgraph of size } k}} \mathbb{E}(X_C) = \frac{|V|}{k+1} a_k (1-p)^m (p(1-p)^{m-2})^k.$$

To prove the second equality we use two lemmas proved below. From Lemma 4.4, the expected value of X_C is $(1-p)^m(p(1-p)^{m-2})^k$, independently of the subgraph C with k edges. Lemma 4.5 guarantees that the number of connected subgraph C is $\frac{|V|}{k+1} a_k$. Finally, the quotient $\frac{|V|}{n}$ is exactly $\frac{2}{m}$. This proves the proposition. □

Lemma 4.4. *Let G be a m-regular graph of girth at least $\delta+2$. If C is a connected subgraph of G with $k \leq \delta$ edges, then C is a connected component of the random graph $G_{\mathcal{E}}$ with probability $(1-p)^m(p(1-p)^{m-2})^k$.*

Proof. If $k = 0$, then C is an isolated point. This component appears in the random graph $G_{\mathcal{E}}$ with probability $(1-p)^m$ by m-regularity of G.

Assume the formula true for every connected subgraph C of size $k-1$, with $k \leq \delta$. A subgraph C of G of size $k-1$ is included in a ball of radius $k-1$. We will prove that the

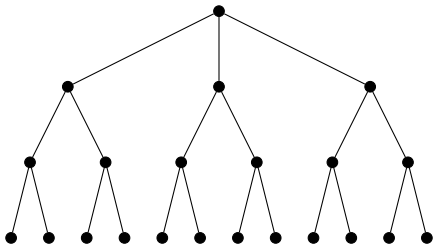

Figure 3: A ball of radius 3 in a 3-regular graph with girth ≥ 7

formula remains true if we add an edge to C. Let x be a vertex of C and let $\{x, y\}$ be an edge which is not in C. Consider the graph $C' = C \cup \{x, y\}$. It contains k edges. Denote by ∂C the set of edges which have exactly one endpoint in C. Similarly, $\partial C'$ is the first neighbourhood of C'. The set $\partial C'$ contains ∂C except $\{x, y\}$. Moreover it contains $m - 1$ new edges: the edges $\{y, z\}$ for $z \neq x$. These edges were not in ∂C. Indeed, if $\{y, z\}$ is included in ∂C, define the graph $C'' = C' \cup \{y, z\}$. It contains $k + 1$ edges and it covers a cycle, because without the edge $\{y, z\}$ it is still connected. This is impossible because the shortest cycle has length at least $\delta + 2$. Thus the formula is satisfied for all $k \leq \delta$. □

Lemma 4.5. *Let G be an m-regular graph of girth at least $\delta + 2$. The number of connected subgraphs of G with $k \leq \delta$ edges is at least:*

$$\frac{|V|}{k+1} a_k.$$

where a_k are the coefficient of the generating function T_m.

Proof. Connected subgraphs with k edges are trees and contain $k + 1$ vertices. It should be clear that given any vertex x, the number of ways of constructing a k-edge subgraph containing x, and hence the number of such subgraphs, is the same in G and in the m-regular tree. □

4.4 Achievable rates

Let $\mathbf{H} = \begin{pmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{pmatrix}$ be the stabilizer matrix of a $(2, m)$ CSS code. Remark that the graphs associated to $\mathbf{H}_X$ and $\mathbf{H}_Z$ have girth at most m, since a row of $\mathbf{H}_Z$ yields a cycle for $\mathbf{H}_X$ and vice versa. We will say that a $(2, m)$ CSS code is proper if the two associated graphs are connected and have girth exactly m.

We now translate the upper bound of Proposition 4.3 into a lower bound on the function $D(p)$ of Theorem 3.5 for a sequence of $(2, m)$ CSS codes.

Proposition 4.6. *For any sequence of proper $(2, m)$ CSS codes we have:*

$$D(p) \geq \Big(\frac{1-2p}{1-p}\Big)\Big(\frac{4}{m} - \frac{4}{m}\big(1 - (1-p)^m S_{m-2}(p(1-p)^{m-2})\big)\Big),$$

where $S_{m-2}(z) = \sum_{k=0}^{m-2} \frac{a_k}{k+1} z^k$ and a_k are the coefficients of the generating function T_m.

Proof. For $\mathbf{H}$ the stabilizer matrix of a proper CSS code, we apply (5) by using for the upper bound $M(p)$ on $\mathbb{E}(\mathrm{rank}(\mathbf{H}_\mathcal{E}))/n$, the sum of the upper bounds provided by Proposition 4.3 on each of the terms $\mathbb{E}(\mathrm{rank}(\mathbf{H}_{X,\mathcal{E}}))/n$ and $\mathbb{E}(\mathrm{rank}(\mathbf{H}_{Z,\mathcal{E}}))/n$. The result follows after some rearranging. □

Finally, Proposition 4.6 together with Theorem 3.5 yields:

Theorem 4.7. *Over the quantum erasure channel of erasure probability p, achievable rates of proper $(2, m)$ CSS codes satisfy*

$$R \leq (1-2p)\Big(\frac{4}{mp}\big(1-(1-p)^m S_{m-2}(p(1-p)^{m-2})\big)-1\Big).$$

where $S_{m-2}(z) = \sum_{k=0}^{m-2} \frac{a_k}{k+1} z^k$ and a_k are the coefficients of the generating function T_m.

5 Erasure threshold of quantum LDPC codes

In this part, we reformulate our bound on achievable rates of quantum LDPC codes by determining an upper bound on the erasure decoding threshold of regular quantum LDPC codes.

The capacity of the quantum erasure channel is $1-2p$. This means that the rate of a family of quantum codes with vanishing decoding error probability over the quantum erasure channel of probability p, satisfies $R \leq 1-2p$. Alternatively, given a family of quantum codes of rate at least R, we can ask for the highest erasure rate that we can tolerate with vanishing error probability after decoding. This is the erasure decoding threshold. Assume that we have a family of quantum codes of rate higher than R, which achieve an asymptotic zero error probability over the quantum erasure channel of erasure probability p. Then, we have:

$$p \leq \frac{1-R}{2}.$$

If we consider CSS codes of type $(2, m)$, we have $2n/m$ rows in each matrix $\mathbf{H}_X$ and $\mathbf{H}_Z$. Therefore, the number of encoded qubits is at least $(1-4/m)n$ (actually it is exactly $(1-4/m)n+2/n$ by Lemma 4.1). Using the bound of Theorem 4.7 and the fact that the rates of the quantum codes are higher than $1-4/m$, we obtain:

Theorem 5.1. *The erasure threshold of $(2, m)$ proper CSS codes is below the solution of the equation:*

$$1-\frac{4}{m} = (1-2p)\Big(\frac{4}{mp}\big(1-(1-p)^m S_{m-2}(p(1-p)^{(\ell-1)(m-1)-1})\big)-1\Big)$$

where $p \in [0, 1/2]$.

This value is obtained at the intersection of the graphical representation of the upper bound with the line $y = 1-4/m$. An example of these curves is given in Figure 4.

Using symbolic computation software, we computed different numerical values of this upper bound on the decoding erasure threshold p_e:

type	improved upper bound on p_e	Capacity bound $p_e \leq 2/m$
$CSS(2,8)$, with Th. 3.8	0.228	0.25
$CSS(2,8)$, with Th. 5.1	0.215	0.25
$Stab(4,8)$, with Th. 3.8	0.228	0.25
$CSS(2,5)$, with Th. 3.8	0.387	0.40
$CSS(2,5)$, with Th. 5.1	0.381	0.40

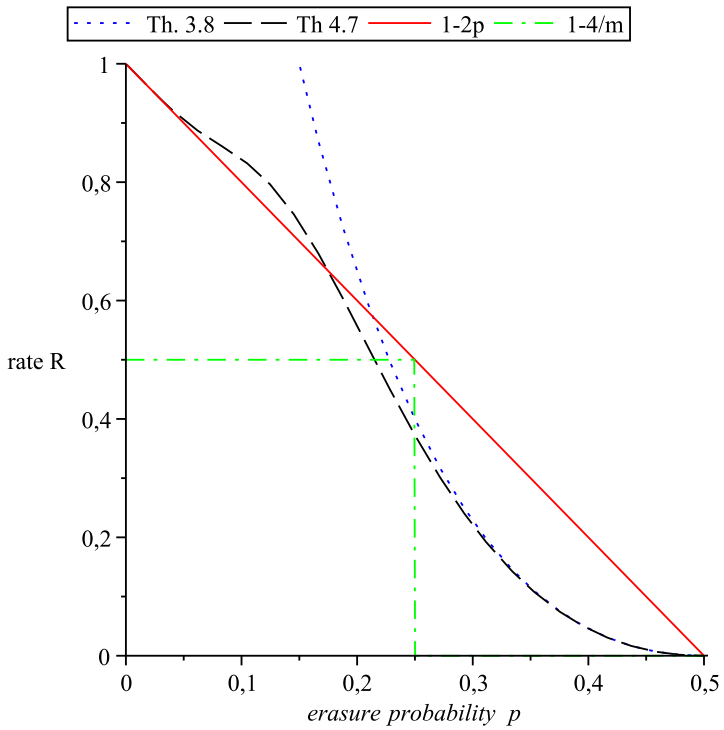

Figure 4: The horizontal green line is the rate of a proper CSS (2,8) code. Its intersection with the capacity gives an upper bound on the erasure threshold of quantum codes : $p_e \leq 0.25$. The two other curves are the upper bounds of Theorems 3.8 and 5.1: their intersection with the horizontal line gives the two upper bounds $p_e \leq 0.228$ and $p_e \leq 0.215$ for CSS (2,8) codes from Theorem 5.1.

6 Application to percolation theory

6.1 Percolation theory

In this section E denotes the edge set of a graph, rather than a Pauli error: context should not allow confusion. Let $G = (V, E)$ be an infinite graph. Denote by μ_p the probability measure on $\{0, 1\}$ defined by $\mu_p(\{1\}) = p$. Consider the product space $\Omega = \{0, 1\}^E$ endowed with the product probability measure $\mathbb{P}_p = \mu_p^{\otimes E}$. Random events should be seen as subgraphs. Informally, we choose every edge of G with probability p independently of the other edges, and obtain a random subgraph. The edges of this subgraph are called *open* edges. Percolation theory is interested in the probability that a given edge e is contained in a infinite open connected component (an open *cluster*). This probability depends a priori on the edge e, but not if the graph G is edge-transitive, for example if G is the infinite square lattice (Figure 5). The central parameter in percolation theory is the *critical probability* p_c, defined as:

$$p_c(G) = \inf\{p \in [0, 1],\ \mathbb{P}_p(|\mathcal{E}(e)| = \infty) > 0\},$$

where $\mathcal{E}(e)$ denotes the open cluster containing edge e.

By a famous result of Kesten [24] that stayed a conjecture for 20 years, we have $p_c = 1/2$ for the square lattice. Computing the critical probability exactly is usually quite difficult.

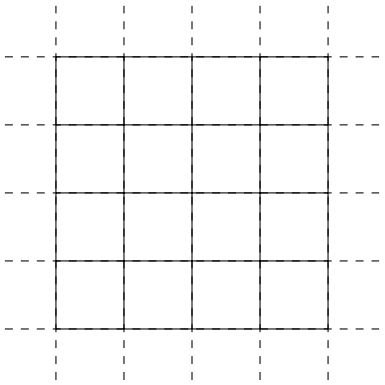

Figure 5: The square lattice

For any integer $m \geq 4$, we denote by $G(m)$ the planar graph which is regular of degree m and tiles the plane by elementary faces of length m. For $m = 4$ the graph $G(4)$ is exactly the square lattice. The local structure of the graph $G(5)$ is shown on Figure 6.

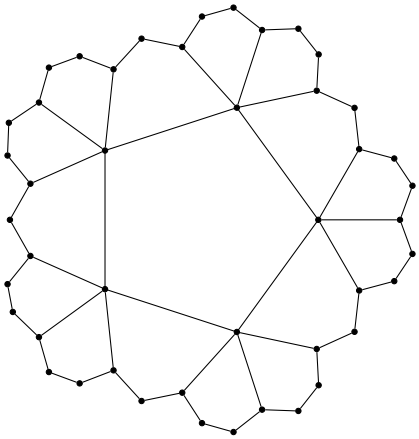

Figure 6: The local structure of the graph $G(5)$

For $m > 4$ these graphs make up regular tilings of the hyperbolic plane. Interest in percolation on hyperbolic tilings was raised in a number of papers e.g. [4, 3, 22] and determining their critical probability $p_c(m)$ is highly non-trivial. Note that all graphs $G(m)$ are self-dual like the square lattice $G(m)$.

We have the following easy bounds on p_c:

Proposition 6.1. *The critical probability p_c of $G(m)$ satisfies*

$$\frac{1}{m-1} \leq p_c.$$

Proof. We adapt the proof of [25] page 14 in the case of the square lattice.

Let O be a fixed vertex. To show the first inequality we can say that there are not more than $m(m-1)^{n-1}$ paths from O of length n in $G(m)$ and the probability of such an open path is p^n. So if $p < \frac{1}{m-1}$ the average length of an open path from O is not more than $\sum_{n=1}^{\infty} m(m-1)^{n-1}p^n < \infty$. In this case p is under the critical probability. □

The same method leads to the upper bound $p_c \leq 1 - \frac{1}{m-1}$. The proof can be immediatly adapte from the case of the square lattice [25] page 14.

6.2 Quotient graphs

To study percolation on the hyperbolic tiling $G(m)$, we need a family of increasingly big finite graphs which are locally the same as $G(m)$. We will use a family introduced by Širáň in [33].

Let $P_k(X) = 2\cos(k \arccos(X/2))$ be the k-th normalized Chebychev polynomial and $\xi = 2\cos(\pi/m^2)$. Let y and z be the matrices of $SL_3(\mathbb{Z}[\xi])$ defined by

$$y = \begin{pmatrix} P_m(\xi)^2 - 1 & 0 & P_m(\xi) \\ P_m(\xi) & 1 & 0 \\ -P_m(\xi) & 0 & -1 \end{pmatrix}$$

$$z = \begin{pmatrix} -1 & -P_m(\xi) & 0 \\ P_m(\xi) & P_m(\xi)^2 - 1 & 0 \\ P_m(\xi) & P_m(\xi)^2 & 1 \end{pmatrix}.$$

These two matrices generate the triangular group $T(m)$ [33]. To obtain a finite graph we can reduce the entries of the matrices modulo a prime number p. The coefficients are in the ring $\mathbb{Z}[\xi]$ which is isomorphic to the quotient $\mathbb{Z}[X]/h(X)$ where h is the minimal polynomial of the algebraic integer ξ. Reducing coefficients modulo p, we obtain a group homomorphism from $SL_3(\mathbb{Z}[\xi])$ to $SL_3(\mathbb{F}_p[X]/(h(X))$. The image of $T(m)$ will be called $\bar{T}(m)$.

Let $\bar{G}(m)$ be the graph defined like $G(m)$ but with the group $\bar{T}(m)$, in other words the vertices, edges and faces of $\bar{G}(m)$ are defined as the left cosets of $\langle \bar{y} \rangle$, $\langle \bar{y}\bar{z} \rangle$ and $\langle \bar{z} \rangle$ respectively. There is a surjection s from $G(m)$ to $\bar{G}(m)$ which sends $u\langle y \rangle$ to $\bar{u}\langle \bar{y} \rangle$.

Following Širáň, let us define the *injectivity radius* of the graph $\bar{G}(m)$ as the largest integer r such that the restriction of the surjection s to a ball of radius r is one-to-one. It is shown in [33] that we can choose p so as to have r arbitrarily large. Loosely speaking, Širáň's argument is that if two distinct vertices $u\langle y \rangle$ and $v\langle y \rangle$ in $G(m)$ have the same image under s then $u^{-1}v$ in $T(m)$ must project to the identity element in $\bar{T}(m)$. But this means that the matrix $u^{-1}v$ has polynomial entries that, properly reduced modulo $h(X)$, can only be expressed with coefficients at least one of which exceeds p: this implies that $u^{-1}v$ can only be expressed as a product of a large number of matrices y and z, which in turn means that the original vertices $u\langle y \rangle$ and $v\langle y \rangle$ have to be far apart in $G(m)$.

The above construction enables us to define a family of finite graphs $(G_r(m))_{r \geq 1}$ such that each graph $G_r(m)$ has injectivity radius at least r, for every integer r.

Let us now define random subgraphs of $G_r(m)$ through the product measure $\mu_p^{\otimes E_r}$, where E_r denotes the edge set of $G_r(m)$. In other words the open subgraph of $G_r(m)$ is created by declaring every edge open with independent probability p.

For any fixed edge e, let $\mathcal{E}_r(e)$ be the (possibly empty) connected component of the random subgraph of $G_r(m)$ that contains e and call it again the open cluster containing e. Let $f_r(p)$ be the probability that $|\mathcal{E}_r(e)| > r$. We have:

Proposition 6.2. *If $p < p_c(m)$ then $f_r(p)$ goes to 0 when r goes to infinity.*

Proof. Notice that the probability $1 - f_r(p)$ that the open cluster containing e has cardinality not more than r is the same for the random subgraph defined on the finite graph $G_r(m)$ and the random subgraph defined on the infinite graph $G(m)$. This is because this event depends

only on the ball of radius r centered on an endpoint of e, and these balls in $G_r(m)$ and $G(m)$ are isomorphic.

We can therefore consider $f_r(p)$ to mean the probability of the event F_r that $|\mathcal{E}(e)| > r$ in the infinite graph $G(m)$. Now $(F_r)_{r\geq 1}$ is a decreasing sequence of events, and $\mathbb{P}_p(\cap_{r\geq 1} F_r)$ is exactly the probability of percolation, which is 0 since we have supposed $p < p_c$. By monotone convergence we therefore have $f_r(p) = \mathbb{P}_p(F_r) \to 0$. □

6.3 The quantum codes $Q_r(m)$ associated with the graphs $G_r(m)$

Every finite graph $G_r(m)$ gives rise to a CSS quantum code $Q_r(m)$ whose coordinate set is the edge set E of the graph. We will have therefore a quantum code of length $n = |E|$. The matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ are defined as described in Section 4.1. The rows of $\mathbf{H}_X$ are in one-to-one correspondence with the vertices of the graph. Every vertex x yields a row of $\mathbf{H}_X$ whose support is exactly the set of edges incident to x. Every row of $\mathbf{H}_X$ therefore has weight m. The rows of the other matrix $\mathbf{H}_Z$ is in one-to-one correspondence with the set of faces of the graph. Every face yields a row whose support is equal to the set of edges making up the face. Since faces are m-gons, every row of $\mathbf{H}_Z$ also has weight m. It should be clear that rows of $\mathbf{H}_X$ and $\mathbf{H}_Z$ meet in either 0 or 2 edges, so any row of $\mathbf{H}_X$ is orthogonal to any row of $\mathbf{H}_Z$ and we have a quantum CSS code of type $(2, m)$.

Recall from Section 4.1 that the classical code C_X is the cycle code of the graph $G_r(m)$. When we reverse the roles of $\mathbf{H}_X$ and $\mathbf{H}_Z$ by declaring the rows of $\mathbf{H}_Z$ (rather than those of $\mathbf{H}_X$) to be vertices and the rows of $\mathbf{H}_X$ to be faces, the graph thus defined is called the dual graph of $G_r(m)$ and we denote it here by $G_r^*(m)$. The classical code C_Z is thus the cycle code of the dual graph $G_r^*(m)$.

From Lemma 4.1, since the graphs $G_r(m)$ and $G_r^*(m)$ are connected, we have:

Proposition 6.3. *The dimension k of the quantum code $Q_r(m)$ equals:*

$$k = \left(1 - \frac{4}{m}\right) n + 2.$$

We remark that for $m = 4$, the graph $G_r(4)$ is a combinatorial torus and the quantum code $Q_r(4)$ is a version of Kitaev's toric code [26]. For $m \geq 5$ the quantum codes $Q_r(m)$ have positive rate bounded away from zero and minimum distance at least $2r$ (see the remark after the proof of Proposition 6.5 below) which is a quantity which behaves as $\log n$. See [37] for a discussion of similar families of surface codes.

Non-correctable erasures. An erasure vector can be identified with a set of edges of $G_r(m)$ (or of $G_r^*(m)$) and we will denote it as before by $\mathcal{E}$. From Proposition 3.1 we have that the erasure pattern $\mathcal{E}$ is non-correctable if and only if $\mathcal{E}$ either contains a cycle of $G_r(m)$ which is not a sum of faces (an element of $C_X \setminus C_Z^\perp$) or $\mathcal{E}$, viewed as a set of edges of the dual graph $G_r^*(m)$, contains a cycle of $G_r^*(m)$ that is not a sum of faces of $G_r^*(m)$ (an element of $C_Z \setminus C_X^\perp$).

6.4 Bounds on the critical probability using the capacity of the quantum erasure channel

Consider an arbitrary member of the family of quantum codes $Q_r(m)$ associated with the graphs $G_r(m)$. Because the original graph $G(m)$ is self-dual, all arguments involving $G_r(m)$ will be seen to hold for its dual graph $G_r^*(m)$ and we will focus on the probability that

the random erasure pattern $\mathcal{E}$ contains a cycle that is not a sum of faces in the original graph $G_r(m)$.

We would like to derive the upper bound on p_c in Theorem 6.8 below by claiming the following: if $p < p_c$, then for the family of graphs $G_r(m)$, the probability that the random set of edges $\mathcal{E}$ contains a cycle which is not a sum of faces vanishes. If this is true, then Theorem 3.5 applies and the rate R of the quantum code $Q_r(m)$ must satisfy $R < 1 - 2p - D(p)$ for every $p < p_c$ and Proposition 6.3 gives the result since $R = 1 - 4/m$.

Unfortunately, we do not know whether for every $p < p_c$, the erasure pattern $\mathcal{E}$ contains no cycle that is not a sum of faces with high probability. What we will prove however, is that if $\mathcal{E}$ contains a cycle that is not a sum of faces, then with high probability one of the representatives of this cycle modulo the space of faces must have very small weight. To violate the capacity of the erasure channel we will therefore use, not $Q_r(m)$ directly, but an "improved" version $Q'_r(m)$ of $Q_r(m)$ that we now introduce.

Proposition 6.4. *Let $Q_r(m)$ be a hyperbolic code, n its length and R its rate. Suppose $\rho \in]0, \frac{1}{2}[$ and $\alpha \in]0, 1[$ are such that*

$$h(\rho) < \alpha < \frac{R}{2},$$

where $h(\rho) = -\rho \log_2 \rho - (1-\rho)\log_2(1-\rho)$ denotes the binary entropy function. Then we can add αn rows to the parity-check matrix $\mathbf{H}_X$ and αn rows to the parity-check matrix $\mathbf{H}_Z$ of $Q_r(m)$ to obtain a CSS code $Q'_r(m)$ of length n, rate $R - 2\alpha$ and distance $d \geq \rho n$.

Proof. Denote by r_X and r_Z the dimension of the code $C_X^\perp$ and $C_Z^\perp$ respectively. We have $r_X = r_Z = \frac{2}{m}n - 1$.

We will construct a matrix $\mathbf{H}'_X$ by adding αn rows to the matrix $\mathbf{H}_X$ such that the rows of $\mathbf{H}'_X$ are orthogonal to the rows of $\mathbf{H}_Z$ and the rank of $\mathbf{H}'_X$ is $r_X + \alpha n$. Let C'_X be the code of parity-check matrix $\mathbf{H}'_X$.

For $\rho \in]0, 1/2[$, we define X_ρ by

$$X_\rho(\mathbf{H}'_X) = |\{v \in C'_X \backslash C_Z^\perp | w(v) \leq \rho n\}|.$$

We can write X_ρ as a sum a random variables to see that

$$\mathbb{E}(X_\rho) = \sum_{\substack{v \in C_X \backslash C_Z^\perp \\ v \in B(0, \rho n)}} \frac{|\{\mathbf{H}'_X | v \in C'_X\}|}{|\{\mathbf{H}'_X\}|}.$$

where $B(0, \rho n)$ denotes the Hamming ball of radius ρn. Let $L_1, L_2, \dots L_{r_X}$ be r_X rows of $\mathbf{H}_X$. The number of suitable matrices $\mathbf{H}'_X$ is the number of families $L'_1, L'_2, \dots L'_{\alpha n}$ of vectors of $\mathbb{F}_2^n$ such that $L'_j \in C_Z$ for all j and $(L_1, L_2, \dots L_{r_X}, L'_1, L'_2 \dots, L'_{\alpha n})$ are linearly independant.

We can construct a suitable matrix $\mathbf{H}'_X$ if and only if $r_X + \alpha n \leq \dim(C_Z)$ this gives the condition $\alpha < (1 - \frac{4}{m}) - \frac{2}{n}$. In this case the number of matrices is

$$\prod_{i=r_X}^{r_X + \alpha n - 1} (2^{n - r_Z} - 2^i).$$

To evaluate the cardinality $|\{\mathbf{H}'_X | v \in C'_X\}|$ with v in $C_X \backslash C_Z^\perp$, it suffices to add the condition $L'_j \in \{v\}^\perp$ for all j. We get

$$\prod_{i=r_X}^{r_X+\alpha n-1} (2^{n-r_Z-1} - 2^i).$$

So we have

$$\frac{|\{\mathbf{H}'_X | v \in C'_X\}|}{|\{\mathbf{H}'_X\}|} = \frac{2^{n-r_X-r_Z-\alpha n}-1}{2^{n-r_X-r_Z}-1} \leq 2^{-\alpha n}.$$

This bound doesn't depend of v so we can give an upper bound on the expectation of X_ρ because we know that the number of words in the ball of radius ρn is less than $2^{nh(\rho)}$. We find

$$\mathbb{E}(X_\rho) \leq 2^{n(h(\rho)-\alpha)}.$$

If $\alpha > h(\rho)$ the mean goes to 0. Since X_ρ has integer values there exists $\mathbf{H}'_X$ such that $X_\rho(\mathbf{H}_X) = 0$. We obtain a CSS code of matrix $\mathbf{H}'_X$ with $r'_X = r_X + \alpha n$ and $\mathbf{H}_Z$ unchanged such that the minimum weight of a word of $C'_X \backslash C_Z^\perp$ is at least ρn.

We want to repeat this argument to have the minimum weight of a word of $C'_Z \backslash C'^\perp_X$ higher than ρn. It suffices to choose $\alpha < \frac{1}{2}(1 - \frac{4}{m}) + \frac{1}{n}$ because in this case $r_Z + \alpha n < \dim(C_X)$. □

Let $\mathcal{E}$ be an erasure. We can write

$$\mathcal{E} = \mathcal{E}_C + \mathcal{E}_P \tag{7}$$

where $\mathcal{E}_C$ is the sum of the connected components which do not cover a cycle which is not a sum of faces. The *problematic* part $\mathcal{E}_P$ of $\mathcal{E}$ is the union of the others components.

In the graph $G_r(m)$, define $g_r(p)$ to be the probability that that the open cluster $\mathcal{E}_r(e)$ covers a cycle which is not a sum of faces. We have:

Lemma 6.5. *If $p < p_c(m)$ then $g_r(p)$ goes to 0 when r goes to infinity.*

Proof. Recall that $f_r(p)$ denotes the probability that $|\mathcal{E}_r(e)| > r$. We prove that $g_r(p) \leq f_r(p)$ and apply Proposition 6.2. If $|\mathcal{E}_r(e)| \leq r$ then the open cluster $\mathcal{E}_r(e)$ is included in a ball of radius r of the graph $G_r(m)$. Since this ball is isomorphic to the ball of the same radius in the planar graph $G(m)$, it is planar. In any planar graph every cycle is a sum of faces so $\mathcal{E}_r(e)$ covers a cycle which is not a sum of faces only if $|\mathcal{E}_r(e)| > r$, hence $g_r(p) \leq f_r(p)$. □

Remark: By the same planarity argument as above, every cycle of length less than $2r$ in the graph $G_r(m)$ is a sum of faces. This proves that the distance of the quantum code $Q_r(m)$ is at least $2r$.

Proposition 6.6. *If we consider the erasure channel of probability $p < p_c$ then $\forall \varepsilon > 0, \exists r_0 \in \mathbb{N}$ such that if $r \geq r_0$ then the expectation of the weight of $\mathcal{E}_P$ defined as in (7) satisfies*

$$\mathbb{E}(|\mathcal{E}_P|) \leq \varepsilon n.$$

Proof. For any edge e of $G_r(m)$, let $X_{r,e}$ be the random variable which take the value 1 if the connected component $\mathcal{E}_r(e)$ of e in $G_r(m)$ covers a cycle which is not a sum of faces and the value 0 otherwise. Then we have:

$$|\mathcal{E}_P| = \sum_e X_{r,e}.$$

To conclude note that $\mathbb{E}(X_{r,e}) = g_r(p)$ and apply Lemma 6.5. □

The next Lemma states that if the erasure vector $\mathcal{E}$ has a large "problematic" part $\mathcal{E}_P$ then it must be correctable by the "improved" codes given by Proposition 6.4.

Lemma 6.7. *Let $Q'_r(m)$ be one of the quantum codes given by Proposition 6.4 and let d be its minimum distance. Suppose the part $\mathcal{E}_P$ of the erasure vector $\mathcal{E}$ defined in* (7) *satisfies $|\mathcal{E}_P| < d$. Then $\mathcal{E}$ is correctable by $Q'(m)$.*

Proof. Denote by C_X and C_Z the binary linear codes associated with the quantum code $Q_r(m)$ and by C'_X, C'_Z their binary sub-codes associated with the quantum code $Q'_r(m)$ introduced in Proposition 6.4 and defined by augmenting the parity-check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ of $Q_r(m)$.

If the erasure vector $\mathcal{E}$ covers an element x of $C'_X \backslash C'^{\perp}_Z$ then x must belong to $C_X \backslash C^{\perp}_Z$ *i.e.* x is a cycle of $G_r(m)$ which is not a sum of faces. The restriction of this cycle to $\mathcal{E}_C$ defined in (7) is another cycle y and the definition of $\mathcal{E}_C$ implies that y is a sum of faces. We obtain that $x + y$ is included in $\mathcal{E}_P$ with $y \in C^{\perp}_Z \subset C'^{\perp}_Z$, i.e. $x + y \in C'_X \backslash C'^{\perp}_Z$ but this is a contradiction whenever the part $\mathcal{E}_P$ of the erasure $\mathcal{E}$ has weight strictly less than the minimum distance d of the improved code $Q'(m)$. □

We are now in a position to give an upper bound on the critical probability of $G(m)$. Recall the definition of the rank difference function of a family of stabilizer codes (Definition 3.4).

Theorem 6.8. *Let $m \geq 5$, and let $p_c(m)$ be the critical probability for percolation on $G(m)$. Let $D(p)$ be the rank difference function of the sequence of stabilizer matrices associated to the tilings $G_r(m)$. Then for any $p < p_c$ we have:*

$$1 - \frac{4}{m} \leq 1 - 2p - D(p).$$

Proof. Let $R = 1 - \frac{4}{m}$ and fix $p < p_c$. For any α such that $0 < \alpha < R/2$, Proposition 6.4 gives us a quantum code $Q'(m)$ with minimum distance $d \geq \rho n$ where $\rho = h^{-1}(\alpha/2)$ and rate $R - 2\alpha$. For such a code the probability of a decoding error satisfies:

$$P_{err} \leq P(|\mathcal{E}_P| \geq \rho n).$$

For any $\varepsilon > 0$ we can take r large enough so that Proposition 6.6 applies, and together with Markov's inequality we have

$$P_{err} \leq P(|\mathcal{E}_P| \geq \frac{\rho}{\varepsilon}\varepsilon n) \leq \frac{\varepsilon}{\rho}.$$

For every $\varepsilon > 0$ we take $\rho = \sqrt{\varepsilon}$. Then $\rho(\varepsilon)$ and $\frac{\varepsilon}{\rho(\varepsilon)}$ simultaneously go to zero when ε goes to zero. Defining α by $\alpha = 2h(\rho)$ and choosing a decreasing sequence of ϵ's that tends to zero, we obtain a family of quantum codes $Q'_r(m)$ with decoding error probability tending to zero and rate $R - 2\alpha$ tending to R.

We can therefore apply Theorem 3.5 to the sequence of stabilizer matrices of the codes $Q'_r(m)$. But we have just seen that their rates tend to $1-4/m$ and furthermore, since the codes $Q'_r(m)$ are obtained from the codes $Q_r(m)$ by adding a vanishing proportion of generators to their stabilizer group, the function $D(p)$ is the same for the family $Q'_r(m)$ as for the family of surface codes $Q_r(m)$. □

Applying the lower bound on $D(p)$ stemming from Proposition 4.6, we obtain after some rearranging:

Theorem 6.9. *We have $p_c(m) \leq p$ where p is the smallest solution $p \in [0,1]$ of the equation:*

$$1 - \frac{4}{m} = (1-2p)\Big(\frac{4}{mp}\big(1-(1-p)^m S_{m-2}(p(1-p)^{m-2})\big) - 1\Big).$$

where $S_{m-2}(x) = \sum_{k=0}^{m-2} \frac{a_k}{k+1} x^k$ and a_k are the coefficients of the generating function T_m.

Using symbolic computation software, we can compute this bound on the critical probability. We use classical properties of generating functions to compute elements of the sequence $(a_k)_k$. For classical theorems on generating functions, in particular Lagrange inversion theorem, see for example [18], [36].

m	lower lower on $p_c(m) : \frac{1}{m-1}$	bound of Th. 6.9	$\frac{2}{m}$ = bound of Prop. 6.1
5	0.25	0.38	0.40
10	0.11	0.16	0.20
20	0.053	0.073	0.100
30	0.035	0.046	0.067
40	0.026	0.033	0.050
50	0.020	0.026	0.040

We can observe that the new upper bound becomes better for tilings m with faces of large length. It is not surprising because, in this case, we enumerate the connected components of larger size.

The exact value of the critical probability remains to discover. Numerical estimations of this value are difficult due to the exponential growth of balls of the graph. For example, Ziff pointed out the inconsistency of some numerical results in [22]. This reinforces the importance of our theoretical approach.

7 Concluding Remarks

- We have given a combinatorial proof of the upper bound on achievable rates of stabilizer codes $R \leq 1-2p$, over the quantum erasure channel. This proof is of course less general than previous proofs, since it applies only to stabilizer codes, but it gives mathematical insight into the degeneracy phenomenon and, as we have shown by the study of sparse stabilizer codes, it has the potential for improved upper bounds on achievable rates for particular classes of quantum codes. A generalization of this approach to the depolarizing channel would be very welcome. The difficulty is the fact that for depolarizing noise the probability of an error depends on its weight. We must deal with typical errors.

- By graphical arguments, we proved that stabilizer and CSS codes defined by generators of bounded weight don't achieve the capacity of the quantum erasure channel. This result can be applied to surfaces codes, color codes and a lot of well studied families of quantum codes. This encourages us to construct irregular quantum LDPC codes and families with growing weights.

- The exact value of the critical probability of hyperbolic tilings remains unknown. To improve our upper bound, we must enumerate more connected components in the random graph, which becomes more difficult when we count components that are not subtrees.

Our method also involves a concavity argument for the mean rank function which relates it to the rank difference function. This results in a manageable lowerbound on the relative rank difference function but it is generally not tight and alternative ways of evaluating this function would be desirable.

Acknowledgement

This work was supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project). We acknowledge support from the Délégation Générale pour l'Armement (DGA) and from the Centre National de la Recherche Scientifique (CNRS). We are very greatful to Jean-François Marckert for helpful discussion around generating functions.

Appendix A: The rank of a random submatrix

The goal of this section is to prove that the function $\phi(p) = \frac{1}{n}\mathbb{E}_p(\operatorname{rank} \mathbf{H}_\mathcal{E})$ is a concave ($\cap$-convex) function. Then, we will use the concavity of ϕ to obtain a lower bound on $\Delta(p) = \phi(1-p) - \phi(p)$.

The key argument is the submodularity of the rank:

Lemma A.1. *Let $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ be a Pauli matrix with n columns. The rank function:*

$$\begin{aligned} \mathcal{P}(\{1,2,\dots,n\}) &\longrightarrow \mathbb{N} \\ A &\longmapsto \operatorname{rank}(A) = \operatorname{rank}(\mathbf{H}_A) \end{aligned}$$

is a submodular function. That is, the rank function satisfies:

$$\operatorname{rank}(A \cap B) + \operatorname{rank}(A \cup B) \leq \operatorname{rank}(A) + \operatorname{rank}(B).$$

This lemma embraces the case of a binary matrix. These rank properties can be obtained in the more general framework of matroid theory. A classical book on matroid theory is [29].

Proof. We will prove the lemma for binary matrices. Then, we will explain how to adapt our argumentation to the quaternary case.

Let A and B be two subsets of $\{1,2,\dots,n\}$. From the dimension formula for the sum of two subspaces, we deduce:

$$\begin{cases} \operatorname{rank}(A \cup B) = \operatorname{rank}(A) + \operatorname{rank}(B\backslash A) - \dim(\operatorname{Im} H_A) \cap (\operatorname{Im} H_{B\backslash A}) \\ \operatorname{rank}(A \cup B) = \operatorname{rank}(B) + \operatorname{rank}(A\backslash B) - \dim(\operatorname{Im} H_B) \cap (\operatorname{Im} H_{A\backslash B}) \\ \operatorname{rank}(A \cap B) = \operatorname{rank}(A) - \operatorname{rank}(A\backslash B) + \dim(\operatorname{Im} H_{A\cap B}) \cap (\operatorname{Im} H_{A\backslash B}) \\ \operatorname{rank}(A \cap B) = \operatorname{rank}(B) - \operatorname{rank}(B\backslash A) + \dim(\operatorname{Im} H_{A\cap B}) \cap (\operatorname{Im} H_{B\backslash A}) \end{cases}$$

Look at the last term of these equalities. We have clearly $\operatorname{Im} H_{A\cap B} \subset \operatorname{Im} H_A$, therefore the space $(\operatorname{Im} H_{A\cap B}) \cap (\operatorname{Im} H_{B\backslash A})$ is a subspace of $(\operatorname{Im} H_A) \cap (\operatorname{Im} H_{B\backslash A})$. This proves the dimension inequality:

$$\dim(\operatorname{Im} H_{A\cap B}) \cap (\operatorname{Im} H_{B\backslash A}) \leq \dim(\operatorname{Im} H_A) \cap (\operatorname{Im} H_{B\backslash A}).$$

We have the same result exchanging A and B. We sum the four equalities and we apply the above inequality. We get the desired result:

$$\operatorname{rank}(A \cap B) + \operatorname{rank}(A \cup B) \leq \operatorname{rank}(A) + \operatorname{rank}(B).$$

To prove the property for a matrix with coefficients in $\mathcal{P}_1$, it is sufficient to show that all the tools from linear algebra used above are still satisfied for a Pauli matrix $\mathbf{H}$. As recalled in Section 2.6, there is an isomorphism of $\mathbb{F}_2$ vector spaces between the Pauli group $\mathcal{P}_n$ and the space $\mathbb{F}_2^{2n}$. Therefore, we can regard the matrix $\mathbf{H} \in \mathcal{M}_{r,n}(\mathcal{P}_1)$ as a matrix $[H^X|H^Z] \in \mathcal{M}_{r,2n}(\mathbb{F}_2)$. The rank function can be written $\operatorname{rank}\mathbf{H} = \operatorname{rank}[H^X|H^Z]$ and the rank of a submatrix is:

$$\operatorname{rank}\mathbf{H}_\mathcal{E} = \operatorname{rank}[H^X_\mathcal{E}|H^Z_\mathcal{E}].$$

From this remark, the proof of the lemma is similar for stabilizer matrices. □

To study the derivatives of ϕ, we introduce the function Φ depending on n variables $x = (x_1, x_2, \ldots, x_n) \in [0,1]^n$ defined by:

$$\Phi(x_1, x_2, \ldots, x_n) = \sum_{\mathcal{E}\in\mathbb{F}_2^n} \left[(\operatorname{rank}\mathbf{H}_\mathcal{E}) \left(\prod_{\mathcal{E}_i=1} x_i \right) \left(\prod_{\mathcal{E}_i=0} (1-x_i) \right) \right].$$

This function can be seen as the expected rank $\mathbb{E}_x(\operatorname{rank}\mathbf{H}_\mathcal{E})$ for the probability measure such that the i-th component of $\mathcal{E}$ is 1 with probability x_i and 0 otherwise, independently of the other components. This polynomial function Φ is infinitely derivable and its partial derivatives satisfy:

Lemma A.2. *For all x in $[0,1]^n$, we have:*

$$\frac{\partial\Phi}{\partial x_i}(x) \geq 0, \qquad \forall i \in \{1,2,\ldots,n\},$$

$$\frac{\partial^2\Phi}{\partial x_i \partial x_j}(x) \leq 0, \qquad \forall i,j \in \{1,2,\ldots,n\}.$$

Proof. Let x be an element of $[0,1]^n$. We remark that Φ is an affine function in each variable. Thus, we have:

$$\begin{aligned}
\frac{\partial\Phi}{\partial x_i}(x) &= \Phi(x_1,\ldots,x_{i-1},1,x_{i+1},\ldots,x_n) - \Phi(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n) \\
&= \mathbb{E}_x(\operatorname{rank}(\mathcal{E}\cup\{i\}) - \mathbb{E}_x(\operatorname{rank}(\mathcal{E}\backslash\{i\}) \\
&= \mathbb{E}_x\Big(\operatorname{rank}(\mathcal{E}\cup\{i\}) - \operatorname{rank}(\mathcal{E}\backslash\{i\}\Big) \\
&\geq 0.
\end{aligned}$$

In the preceding expression, the vector $\mathcal{E} \in \mathbb{F}_2^n$ is considered as a subset of $\{1,2,\ldots,n\}$. Fixing $x_i = 1$ is equivalent to replacing the subset $\mathcal{E}$ by $\mathcal{E}\cup\{i\}$ and fixing $x_i = 0$ is equivalent to considering the subset $\mathcal{E}\backslash\{i\}$.

Let j be an integer between 1 and n such that $j \neq i$. The partial derivative $\frac{\partial\Phi}{\partial x_i}(x)$ is also an affine function of the j-th variable thus we can derivate it by the same process. We find:

$$\begin{aligned}
\frac{\partial^2\Phi}{\partial x_j\partial x_i}(x) &= \frac{\partial}{\partial x_j}\frac{\partial\Phi}{\partial x_i}(x) \\
&= \mathbb{E}_x(\operatorname{rank}(\mathcal{E}\cup\{i,j\})) - \mathbb{E}_x(\operatorname{rank}(\mathcal{E}\cup\{i\}\backslash\{j\})) \\
&- \mathbb{E}_x(\operatorname{rank}(\mathcal{E}\cup\{j\}\backslash\{i\})) + \mathbb{E}_x(\operatorname{rank}(\mathcal{E}\backslash\{i,j\})) \\
&= \mathbb{E}_x\left[\operatorname{rank}(A_i\cup A_j) - \operatorname{rank}(A_i) - \operatorname{rank}(A_j) + \operatorname{rank}(A_i\cap A_j)\right] \\
&\leq 0.
\end{aligned}$$

The subset A_i denotes the subset $\mathcal{E} \cup \{i\} \backslash \{j\}$ and A_j denotes the subset $\mathcal{E} \cup \{j\} \backslash \{i\}$. This quantity is negative by the submodularity of Lemma A.1

If $j = i$ then the second partial derivative is null. □

Proposition A.3. *Let $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ be a Pauli matrix with n columns. The function $\phi(p) = \frac{1}{n}\mathbb{E}_p(\operatorname{rank} \mathbf{H}_\mathcal{E})$ is an increasing function on $[0, 1]$.*

Proof. The function ϕ is $\frac{1}{n}\Phi \circ i$ where i is the injection from $[0, 1]$ to $[0, 1]^n$ which sends p onto $(p, p \ldots, p)$. The derivatives of ϕ can be expressed as function of the partial derivatives of Φ:

$$\phi'(p) = \frac{1}{n} \sum_{i=1}^{n} p \frac{\partial \Phi}{\partial x_i}(i(p)).$$

From Lemma A.2, this number is always non-negative. □

Proposition A.4. *Let $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ be a Pauli matrix with n columns. The function $\phi(p) = \frac{1}{n}\mathbb{E}_p(\operatorname{rank} \mathbf{H}_\mathcal{E})$ is a concave function on $[0, 1]$.*

Proof. With the same notation as in the proof of Proposition A.3, we obtain:

$$\phi''(p) = \frac{1}{n} \sum_{i,j=1}^{n} p^2 \frac{\partial^2 \Phi}{\partial x_i \partial x_j}(i(p))$$

From Lemma A.2, this number is always non-positive, proving the concavity of ϕ. □

Proposition A.5. *Let $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ be a Pauli matrix with n columns. Assume that $\phi(p) = \frac{1}{n}\mathbb{E}_p(\operatorname{rank} \mathbf{H})$ is upper bounded by $M(p)$. Then, the function $\Delta(p) = \phi(1 - p) - \phi(p)$ admits the lower bound:*

$$\Delta(p) \geq \left(\frac{1 - 2p}{1 - p}\right) \left(\frac{\operatorname{rank} \mathbf{H}}{n} - M(p)\right)$$

Proof. It suffices to use the concavity of f. Indeed, by concavity the point $(1 - p, \phi(1 - p))$ is above the segment between $(p, \phi(p))$ and $(1, \phi(1))$. That is:

$$\phi(1 - p) \geq \phi(p) + (1 - 2p) \left(\frac{\phi(1) - \phi(p)}{1 - p}\right).$$

The inequality follows using the equality $\phi(1) = \operatorname{rank} \mathbf{H}/n$ and then the upper bound $\phi(p) \leq M(p)$. □

References

[1] S.A. Aly. A class of quantum LDPC codes derived from latin squares and combinatorial objects. Technical report, Department of Computer Science, Texas A and M University, 2007.

[2] S.A. Aly. A class of quantum LDPC codes constructed from finite geometries. In *Proc. of Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008*, pages 1–5, dec. 2008.

[3] S. K. Baek, P. Minnhagen, and B. J. Kim. Percolation on hyperbolic lattices. *Phys. Rev. E* 79:011124, 2009.

[4] I. Benjamini and O. Schramm. Percolation beyond $\mathbb{Z}^d$, many questions and a few answers. *Electr. Commun. Probab*, 1:71–82, 1996.

[5] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin. Capacities of quantum erasure channels. *Phys. Rev. Lett.*, 78:3217–3220, 1997.

[6] C. Berge. *Graphs and Hypergraphs*. Elsevier, 1976, 1973.

[7] H. Bombin and M. A. Martin-Delgado. Topological quantum distillation. *Phys. Rev. Lett.*, 97:180501, 2006.

[8] H. Bombin and M. A. Martin-Delgado. Exact topological quantum order in $d = 3$ and beyond: Branyons and brane-net condensates. *Phys. Rev. B*, 75:075103, 2007.

[9] H. Bombin and M. A. Martin-Delgado. Homological error correction: Classical and quantum codes. *J. Math. Phys.*, 48(5):052105, 2007.

[10] D. Burshtein, M. Krivelevich, S. Litsyn, and G. Miller. Upper bounds on the rate of LDPC codes. *IEEE Trans. on Information Theory*, 48:2437–2449, 2002.

[11] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996.

[12] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $GF(4)$. *IEEE Trans. on Information Theory*, 44(4):1369 –1387, jul 1998.

[13] T. Camara, H. Ollivier, and J-P. Tillich. A class of quantum LDPC codes: construction and performances under iterative decoding. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2007*, pages 811 –815, june 2007.

[14] A. Couvreur, N. Delfosse, and G. Zémor. A construction of quantum LDPC codes from Cayley graphs. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2011*, pages 643 –647, 31 2011-aug. 5 2011.

[15] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, August 1991.

[16] N. Delfosse and G. Zémor. Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane. In *Proc. of IEEE Information Theory Workshop, ITW 2010*, pages 1–5, sept. 2010.

[17] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. Math. Phys.*, 43:4452, 2002.

[18] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 1 edition, 2009.

[19] R. Gallager. *Low Density Parity-Check Codes*. PhD thesis, Massachusetts Institute of Technology, 1963.

[20] M. Grassl. Algorithmic aspects of quantum error-correcting codes. In Ranee K. Brylinski and Goong Chen, editors, *Mathematics of Quantum Computation*, pages 223–252. Chapman and Hall/CRC, 2002.

[21] M. Grassl, T. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56:33–38, Jul 1997.

[22] H. Gu and R. M. Ziff. Crossing on hyperbolic lattices, 2011. `http://arxiv.org/abs/1111.5626`

[23] M. Hagiwara and H. Imai. Quantum quasi-cyclic LDPC codes. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2007*, pages 806 –810, june 2007.

[24] H. Kesten. The critical probability of bond percolation on the square lattice equals 1/2. *Communications in Math. Phys.*, 74:41–59, 1980.

[25] G. Grimmett, *Percolation*. Springer-Verlag, 1989.

[26] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Phys.*, 303(1):27, 1997.

[27] D.J.C. MacKay, G. Mitchison, and P.L. McFadden. Sparse-graph codes for quantum error correction. *IEEE Trans. on Information Theory*, 50(10):2315 – 2330, oct. 2004.

[28] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 1 edition, 2000.

[29] J. G. Oxley. *Matroid Theory*. Oxford University Press, New York, 1992.

[30] J. Preskill. Quantum information and computation, 1998. `http://www.theory.caltech.edu/people/preskill/ph229/`

[31] T. Richardson and R. Urbanke. *Modern Coding Theory*. Cambridge University Press, 1 edition, 2008.

[32] K.P. Sarvepalli, M. Rötteler, and A. Klappenecker. Asymmetric quantum ldpc codes. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2008*, page 305–309, July 2008.

[33] J. Širáň. Triangle group representations and constructions of regular maps. *Proc. of the London Mathematical Society*, 82(03):513–532, 2000.

[34] A. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. Lond. A*, 452:2551, 1996.

[35] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$;. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2009*, pages 799 –803, july 2009.

[36] H. S. Wilf. *Generatingfunctionology*. A. K. Peters, Ltd., Natick, MA, USA, 2006.

[37] G. Zémor. On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In *Proc. of the 2nd International Workshop on Coding and Cryptology, IWCC '09*, pages 259–273, Berlin, Heidelberg, 2009. Springer-Verlag.